

ANATOMY OF RUSSIA'S 2016 INFLUENCE OPERATIONS:

HACKS, LEAKS, AND THE
MANIPULATION OF POLITICAL OPINION

The following is derived from open source collection. None of the data used in this report has come from Mandiant incident response investigations or other privileged access to FireEye customer data.

FireEye takes seriously its obligations to client confidentiality and data privacy.

CONTENTS

Introduction	4	Part Two: Attribution	50
Executive Summary	6	Assessment 3	51
Part One: False Hactivist Personas	12	Section 2.1: Overlaps with APT28	53
Assessment 1	13	Section 2.2: Other Indications of Russian Operator Involvement	60
Brands Appropriated by Suspected Russian False Hactivist Personas	14	Section 2.3: Additional Overlaps between Personas	63
Section 1.1: Guccifer 2.0	15	Part Three: Dissemination	65
Guccifer 2.0 Timeline of Activity	17	Assessment 4	66
Section 1.2: DC Leaks	19	Assessment 5	67
DC Leaks Timeline of Activity	21	Section 3.1: Platforms	68
Section 1.3: @anpoland (Anonymous Poland)	22	3.1.1: Twitter Accounts	69
@anpoland Timeline of Activity	26	3.1.2: Dedicated Websites	70
Section 1.4: Fancy Bears' Hack Team	27	3.1.3: WikiLeaks	71
Fancy Bears' Hack Team Timeline of Activity	30	WikiLeaks Timeline of Activity	72
Section 1.5: @pravsector	31	Section 3.2: Direct Advocacy	74
@pravsector Timeline of Activity	34	Section 3.3: Indirect Advocacy via Warlists	77
Section 1.6: Bozkurt Hackers (aka Hacker Buba)	35	3.3.1: What are Warlists? The Example of @anpoland and the #WarAgainstDemocrats	78
Bozkurt Hackers Timeline of Activity	38	3.3.2: Overview of Identified Warlist Activity and Aims	83
Section 1.7: Other Personas	39	3.3.3: Warlist Account Characteristics	92
Assessment 2	40	Appendix: Timeline of Activity	109
1.7.1: CyberCaliphate	41		
CyberCaliphate Timeline of Activity	44		
1.7.2: CyberBerkut	45		
CyberBerkut Timeline of 2016-2017 Activity	48		

Over the past year and a half, FireEye iSIGHT Intelligence has conducted an in-depth investigation of Russian influence operations conducted during 2016.

This three-part report details our main findings. The scope of Russia's influence activity in 2016 was far-reaching. Our aim in producing this report now, in 2017, despite some aspects of the activity having occurred over a year ago, is to help unmask some of the layers of Russia's influence machinery and demonstrate the linkages between seemingly disparate incidents of cyber threat activity. We hope this will promote greater understanding of the full extent of what occurred, such that similar efforts in future might be better identified and mitigated. FireEye iSIGHT Intelligence reported on much of the activity discussed in this report as it occurred. We here build upon that with further investigative work we have carried out, and where suitable, draw upon and reference some of the excellent public analysis published by other security researchers and journalists.

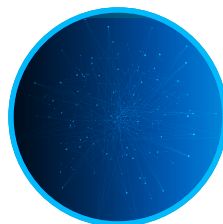
Part One of our investigation details the activities and purported identities of six false hacktivist personas that we assess Russia leveraged for influence operations in 2016: Guccifer 2.0, DC Leaks, Anonymous Poland (@anpoland), Fancy Bears' Hack Team, @pravsector, and Bozkurt Hackers. We also provide background on two other personas, CyberCaliphate and CyberBerkut, that we have previously assessed were also leveraged by Russia for information operations.



Part Two details why we assess the six personas to have been Russian Government-sponsored, outlining their connections to the Russian cyber espionage group APT28, the presence of other indications of Russian operator affiliation, and the shared behavioral characteristics across some of the personas that suggest them to be related.



Part Three provides a detailed analysis of some of the dissemination methods the personas employed to promote their cyber threat activity and associated political narratives. Included in this section is a discussion on the use of WikiLeaks to disseminate DNC and Clinton campaign chairman John Podesta's emails, as well as detailed dissections of manual and semi-automated Twitter-based promotional activity that was carefully orchestrated to inject news of leaks and associated narratives into specific audiences and communities from which they might then organically proliferate.



A detailed timeline of all relevant threat activity and developments that occurred over the course of 2016 is presented as an appendix.

Executive Summary



Russian state-sponsored
actors leveraged
at least six false
hactivist personas



over the course of

2016

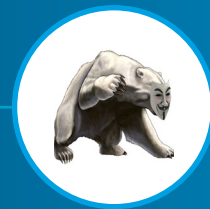
Part One: False Hactivist Personas

We assess, with varying respective degrees of confidence, that Russian state-sponsored actors leveraged at least six false hactivist personas over the course of 2016 to conduct a series of information operations designed to further Russian political interests. Each of these personas engaged in what we term “brand appropriation,” appropriating pre-existing hactivist or political brands to obfuscate their true origins and to generate publicity and impressions of credibility



These personas were:

- Guccifer 2.0 (high confidence in Russian sponsorship)
- DC Leaks (high confidence in Russian sponsorship)
- Anonymous Poland/@anpoland (high confidence in Russian sponsorship)
- Fancy Bears' Hack Team (high confidence Russian sponsorship)
- Pravyi Sector/@pravsector (high confidence in Russian sponsorship)
- Bozkurt Hackers (moderate confidence in Russian sponsorship)



The best known of these personas, **Guccifer 2.0** and **DC Leaks**, claimed to leak data with the intent to influence perceptions and shape attitudes around the November 2016 US elections. We believe that the primary goal of this activity was to undermine confidence in the electoral process among the American populace and to exacerbate existing political divisions, with aspirations that this would undermine the projection of US power abroad, and distract US attention away from Russia's political and military pursuits elsewhere in the world. In material terms, this predominantly took the form of a concerted effort to discredit the candidacy of Hillary Clinton through leaks of documents and emails designed to portray the former Secretary of State and the Democratic Party as corrupt and unfit for political office.

The **@anpoland** persona likewise engaged in influence activity targeting the US elections, leaking documents – including some that were fabricated – from The Bradley Foundation, a US-based conservative non-profit, and engaging in a carefully orchestrated and systematized social media campaign to use the leak to portray Clinton as corrupt. Additionally, the **@anpoland** persona claimed or threatened to engage in threat activity, including DDoS attacks and data leaks, against Ukrainian entities as well as organizations involved in the enforcement of anti-doping regulations during the 2016 Olympic games, including the Court of Arbitration for Sport (CAS) and World Anti-Doping Agency (WADA).

That latter organization, WADA, was the victim of a sustained influence campaign by the **Fancy Bears' Hack Team** persona, which, beginning in Fall 2016, released medical records detailing authorized therapeutic exemptions for the use of otherwise banned substances by numerous high-profile athletes. These leaks, intended to portray WADA as facilitating doping by Western athletes, followed the ban of Russian competitors from the 2016 Olympic and Paralympic games due to Russia's own extensive doping operation. The persona also purportedly leaked documents from the Canadian Centre for Ethics in Sport (CCES) and the US Anti-Doping Agency (USADA).



The **@pravsector** persona, falsely portraying itself as affiliated with the Ukrainian nationalist group Right Sector, claimed to leak data from Polish targets including Polish telecom Netia and the Polish Ministry of Defense, in what we believe was an effort to undermine Polish-Ukrainian relations and Poland's relationship with NATO ahead of the 2016 NATO Warsaw Summit. As part of their activities, the @pravsector and @anpoland personas directly interacted with one another in an apparent attempt to further inflame animosities between Ukraine and Poland, engaging in "retaliatory" exchanges of cyber threat activity.



Finally, the **Bozkurt Hackers** persona, falsely presenting itself as a hacker group aligned with the Turkish nationalist organization Grey Wolves, claimed to leak data from numerous banks in the Middle East and South Asia in 2016. The most prominent incident was the leak of data from Qatar National Bank (QNB), which was accompanied by political messaging that, among other themes, called negative attention to the Qatari royal family and Qatari security institutions – political themes that contrasted sharply with Turkish interests and Turkey's collaborative relationship with Qatar. At the time of the leak, Qatar and Turkey both supported Syrian fighters opposing the regime of Russia's ally Bashar al-Assad. Additionally, Grey Wolves fighters were reported to be defending ethnic Turkmen Syrians against Assad regime and Russian military offensives. A Grey Wolves fighter was also reportedly responsible for killing the pilot of a Russian fighter jet that was shot down by Turkey in November 2015 along its southern border with Syria. Anecdotal evidence also suggests that Grey Wolves members traveled to the border area between Crimea and Ukraine's Kherson Oblast to visit prominent members of the Crimean Tatar community, to the apparent consternation of commentators in Russia.



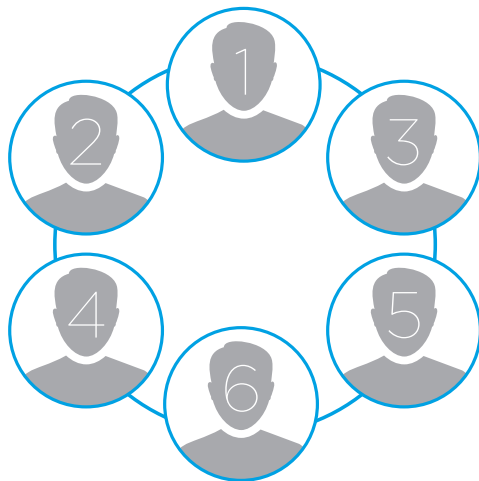
Russia's use of hacker personas to support information operations was not new in 2016. FireEye iSIGHT Intelligence has previously assessed that the **CyberCaliphate** and **CyberBerkut** personas were deployed to support Russian influence campaigns beginning in 2014.

The **CyberCaliphate** persona, which falsely portrayed itself as being a pro-Islamic State (ISIS) hacker group, is best known for its destructive attack against French television station TV5Monde in April 2015, as well as the compromise of social media accounts belonging to US Central Command (CENTCOM).

The **CyberBerkut** hacker group first emerged in 2014 following the Ukrainian Maidan protests, and has conducted extensive cyber threat activity related to the ongoing military conflict between Russia and Ukraine in the Donbass region and Crimea, against targets ranging from Ukrainian Government officials and organizations to NATO and the governments of Germany, Poland, and the United States. Russia's 2016 influence activity represents an expansion and evolution of this historical activity rather than a new phenomenon.

Part Two: Attribution

Our assessment that the influence activity conducted by the six false personas in 2016 was Russian state-sponsored is based on its overlap with intrusion activity conducted by the Russian cyber espionage group APT28, other technical and circumstantial indications of Russian operators behind individual incidents, and uncanny similarities in the promotional behavior of the personas that tie them together.



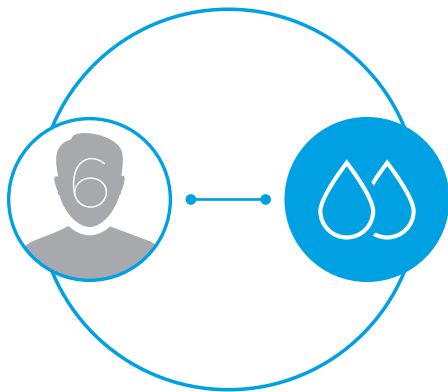
Overt activity conducted by the Guccifer 2.0, DC Leaks, @anpoland, and Fancy Bears' Hack Team personas overlaps directly with covert intrusion and other malicious activities that FireEye and other security companies have attributed to the Russian cyber espionage group we track as APT28. We do not imply that the APT28 intrusion operators are the same operators behind the personas and their public-facing activity. Given the economics of resource allocation and the disparate skillsets employed, we suspect that these functions were likely segregated, with the actors responsible for compromising systems and obtaining sensitive data passing this on to a separate set of actors specializing in curation and dissemination. However, we do not have further insight into the specific entity or entities tasked with this dissemination function.

Connections to APT28 are weaker with regards to the @pravsector and Bozkurt Hackers personas; however, other indications point to Russian-speaking actors having been responsible for obtaining the data those personas subsequently leaked. One hypothesis we are currently exploring is that the intrusion operators that provided data to @pravsector and Bozkurt Hackers are an example of the often blurred boundary between official government actors and criminal actors coopted by the state. Uncanny similarities in leak dissemination behavior between the @anpoland, Fancy Bears' Hack Team, @pravsector, and Bozkurt Hackers personas lead us to assess that all four were controlled by the same actor(s) (see Part Three). Collectively, we suggest, this is indicative of a centralized information operations apparatus collating and disseminating data obtained via multiple intrusion operators.

Part Three: Dissemination

We assess with high confidence that the personas engaged in highly organized, systematized, and in some cases semi-automated social media dissemination campaigns to promote leaks and associated political narratives to media outlets and other influencers, in order to generate mainstream coverage and public attention.

This dissemination activity included what we have termed **Direct Advocacy**, whereby the personas directly targeted influential individuals such as journalists with promotional messaging, and **Indirect Advocacy via “Warlists,”** whereby large networks of semi-automated Twitter accounts, presenting as unaffiliated with the personas, similarly pushed leaks and associated



narratives to influential individuals in a highly systematized manner via targeted messaging. We suggest that this advocacy demonstrated, to at least some degree, a nuanced understanding of the personas' target audiences. All six of the personas in 2016 engaged in some form of direct advocacy. Four of the personas – @anpoland, Fancy Bears' Hack Team, @pravsector, and Bozkurt Hackers – engaged in strikingly similar instances of indirect advocacy via the use of Twitter Warlists.

We have defined the “Warlist” moniker to mean cultivated networks of human-assisted bots (or “cyborg” accounts) designed to produce large-scale bursts of customized, politically-motivated messaging following inputs from a human operator. These Warlists exhibited several characteristics that we believe qualify them as a unique subset of bot activity, including the universal adoption of identical false identities – particularly those of media entities – by accounts within individual Warlists, and the organized manner of their promotional activity, with accounts posting thousands of times in alphabetical order following consistent schedules.

We assess with high confidence that the operators behind the Guccifer 2.0 and DC Leaks personas also leveraged WikiLeaks in their effort to undermine Hillary Clinton's presidential campaign and the Democratic Party more broadly.

From the summer of 2016 through to US election day on November 8, the anti-secrecy organization WikiLeaks released thousands of documents purportedly stolen from the Democratic National Committee and the personal email account of Clinton campaign chairman John Podesta. These releases fed the proliferation of numerous narratives regarding a “corrupt” Hillary Clinton and disinformation intended to undermine her candidacy. We are unable to make a clear determination as to whether WikiLeaks knowingly and willingly colluded with Russia in these leaks, or was an unwitting partner that was passed the allegedly stolen data by a purported unaffiliated intermediary. Regardless of the nature of the relationship, WikiLeaks' statements and rhetoric indicate that the organization willingly and enthusiastically leaked data with the intention of undermining Clinton's presidential campaign. We assess that Russia opted to also leverage WikiLeaks as a publication vehicle due to the organization's high profile and perceived credibility.

Part One: False Hacktivist Personas

Assessment 1

We assess, with varying respective degrees of confidence, that Russian state-sponsored actors leveraged at least six false hacktivist personas over the course of 2016 to conduct a series of information operations designed to further Russian political interests. Each of these personas engaged in what we term “brand appropriation,” appropriating pre-existing hacktivist or political brands to obfuscate their true origins and to generate publicity and impressions of credibility.




BRANDS APPROPRIATED BY SUSPECTED RUSSIAN FALSE HACKTIVIST PERSONAS

Each persona appropriated a pre-existing hacktivist or political brand and used similar images, names, and/or rhetoric to associate with another entity's identity and reputation. This tactic served to hide the true identity of the operators behind the personas, provide plausible deniability, and take advantage of existing preconceptions about these brands for the purposes of publicity, the perception of credibility, and in some cases, to willfully misattribute blame.

PERSONA	BRAND	DESCRIPTION
	Guccifer	Infamous hacktivist actor
	WikiLeaks	Leak organization
	Anonymous	Hacktivist collective
	Anonymous Fancy Bear	Hacktivist collective CrowdStrike name for APT28
	Right Sector	Ukrainian nationalist political/ paramilitary group
	Grey Wolves	Turkish nationalist political/paramilitary group

**Section 1.1:
Guccifer 2.0**



**GUCCI
FER2.0**

Period of Activity:
JUNE 2016 – JANUARY 2017

Appropriated Brand:
GUCCIFER (ROMANIAN HACKER MARCEL LAZĂR)

Blog:
GUCCIFER2.WORDPRESS.COM

Activity:
DATA LEAKS

Confidence in Russian State Sponsorship:
HIGH

Guccifer 2.0 surfaced on June 15, 2016, the day after the security firm CrowdStrike published its report attributing compromises at the Democratic National Committee (DNC) to the intrusion groups FireEye tracks as APT28 and APT29.¹ The Guccifer 2.0 persona attempted to portray itself as a Romanian hacktivist motivated by ego and a vague populist, anti-corruption ideology, similar to the original “Guccifer,” Marcel Lazăr.² Lazăr is a Romanian hacktivist known for compromising the email accounts of high profile US Government figures including Gen. Colin Powell, Hillary Clinton advisor Sidney Blumenthal, and members of the Bush family, and has been serving a prison sentence in Romania since January 2014.³

From June to November 2016, Guccifer 2.0 leaked hundreds of documents purportedly stolen from the DNC and the Democratic Congressional Campaign Committee (DCCC).⁴ We concur with the US Intelligence Community's assessment that the operators behind the Guccifer 2.0 persona also likely provided documents purportedly stolen from the DNC and Democratic officials to WikiLeaks, based on both Guccifer 2.0's public claims and WikiLeaks' July 22, 2016 release of what appear to be nearly 20,000 genuine Democratic Party emails and attachments (See Figure 1.1.1).⁵

We also assess with moderate confidence that the Guccifer 2.0 persona, on at least one occasion, lied about the source of leaked documents and altered data prior to release. On October 4, 2016, the persona claimed to have obtained documents through a compromise of the Clinton Foundation and, we suspect, created a folder in that data dump titled “Pay to Play,” a reference to the at-the-time widely parroted accusation that the Clinton Foundation had accepted foreign donations in exchange for political access to Hillary Clinton while she was Secretary of State. The “Pay to Play” folder contained, among other documents, an email titled “pay-to-play update,” the content of which included the contents of Figure 1.1.2, and other text.

The folder also contained five Microsoft Word documents that also mentioned the Pay to Play phrase in various contexts. On the same day, Russian state media outlet RT published an article titled “New Guccifer 2.0 claims: Hacked Clinton Foundation files show ‘pay to play’, bank ties,” and prominently highlighted the Pay to Play folder.⁶ Referencing this leak, the Guccifer 2.0 blog additionally stated that “It looks like big banks and corporations agreed to donate to the Democrats a certain percentage of the allocated TARP [Troubled Asset Relief Program] funds.”

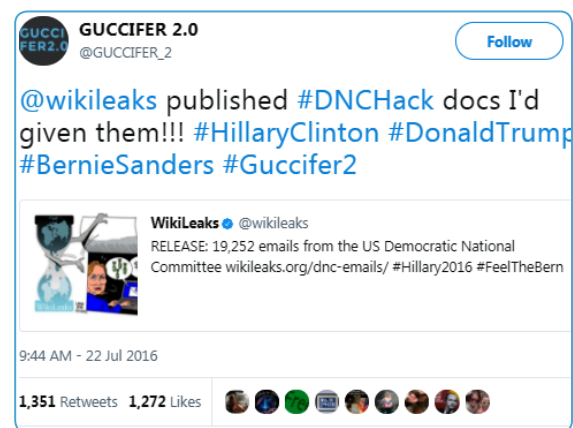


FIGURE 1.1.1: GUCCIFER 2.0 CLAIMS TO HAVE PROVIDED WIKILEAKS WITH LEAKED DNC E-MAILS

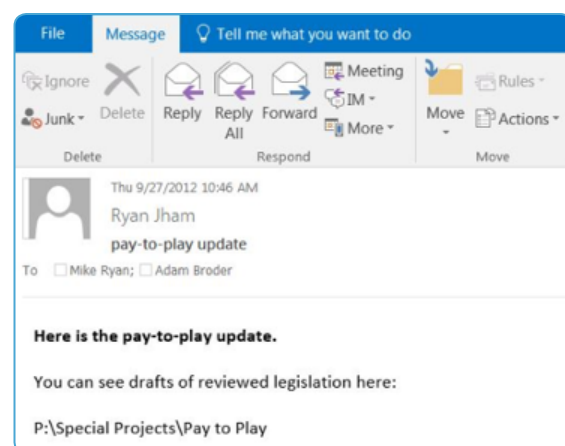


FIGURE 1.1.2: SCREENSHOT OF SUSPECTED ALTERED EMAIL REFERENCING “PAY TO PLAY”

¹ <https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/>

² https://motherboard.vice.com/en_us/article/dnc-hacker-guccifer-20-full-interview-transcript

³ <http://www.bbc.com/news/world-us-canada-37250907>

⁴ <https://www.nytimes.com/2016/12/13/us/politics/house-democrats-hacking-dccc.html>

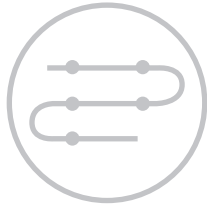
⁵ https://www.dni.gov/files/documents/ICA_2017_01.pdf

⁶ <https://www.rt.com/usa/361608-clinton-foundation-hacked-guccifer/>

Donna Shalala, President of the Clinton Foundation, denied that the organization had been compromised, stating that “...none of the files or folders shown are ours,” and FireEye iSIGHT Intelligence noted at the time that some of the files’ metadata referenced authors associated with the DCCC, suggesting that the DCCC was likely the source of the leaked materials.⁷ Our suspicion that the Pay to Play references were fabricated stems from their impeccable timing, which coincided with extensive use of the term in negative political discourse regarding Clinton, the low likelihood that the Clinton Foundation would directly

reference that specific term in documents even if the allegations were true, and the incongruous use of the term within the leaked documents, with disjointed statements such as “the timing of some of the donations show potential for pay to play” and “timing is also an issue, as several telecom companies gave to Denham at dates that show potential pay to play.” We suspect the Pay to Play content was thus added to further inflame politicized narratives alleging Clinton corruption; however, we defer to investigators with access to the original documents to make a stronger determination.

TIMELINE OF ACTIVITY



2016

JUN 15

Guccifer 2.0 leaks data allegedly stolen from the DNC via a dedicated blog and directly leaks to media outlets The Hill, The Smoking Gun, and Gawker

JUN 18

Guccifer 2.0 leaks additional DNC documents, including financial reports and donors’ personally identifiable information (PII)

JUN 20

@Guccifer_2 Twitter account created, links to the Guccifer 2.0 WordPress site

JUN 21

Guccifer 2.0 leaks alleged DNC files on Hillary Clinton including memos, defensive strategies regarding issues including Clinton’s classified email scandal, expense lists, and donor lists

JUL 6

Guccifer 2.0 leaks additional alleged DNC documents including the DNC action plan for the Republican National Convention, a May 16, 2016 “Event Memo” detailing logistics for President Obama’s appearance at a May 18 DNC fundraising event in Washington D.C, a DNC LGBT event guest list, and donor information

JUL 13

Guccifer 2.0 leaks alleged DNC data to The Hill, including files related to controversial donors and research on Sarah Palin; documents are subsequently posted publicly to the Guccifer 2.0 blog on July 14

JUL 14

Guccifer 2.0 leaks additional alleged DNC documents, including data on contributions from Norman Hsu (the convicted pyramid investment promoter who was previously a fundraiser for the Democratic party), opposition research on Sarah Palin, and additional donor information

JUL 18

Guccifer 2.0 leaks second set of alleged DNC data exclusively to The Hill, including files regarding “political strategies, the upcoming Democratic National Convention and fundraising”⁸

⁷ <https://twitter.com/donnashalala/status/783414514259636224>

⁸ <http://thehill.com/policy/cybersecurity/288119-new-guccifer-20-dump-highlights-wobbly-dems-on-iran-deal>

JUL 22

WikiLeaks posts 20,000 alleged DNC emails; Guccifer 2.0 claims on Twitter to have provided the documents to WikiLeaks⁹

AUG 12

Guccifer 2.0 claims to leak data from the DCCC; some content subsequently removed from the persona's WordPress blog, including database of contact information for Democratic Members of Congress and lists of passwords seemingly for subscription resources and social media accounts used by DCCC staff¹⁰

AUG 15

Guccifer 2.0 leaks alleged DCCC data regarding primaries in Florida, including briefings, memos, and files on primarily Democratic candidates. Documents on at least one Republican candidate, John Mica, are also present

AUG 21

Guccifer 2.0 leaks alleged DCCC data regarding primaries in Pennsylvania, including memos and press statements about the candidates, and background research on the candidates and Pennsylvania's political climate

AUG 23

Guccifer 2.0 leaks alleged DCCC data exclusively to The Hill; documents include DCCC research, campaign strategies, and polling information on Pennsylvania's contested primary for House seats¹¹

AUG 31

Guccifer 2.0 claims to leak documents purportedly taken from Nancy Pelosi's computer, including documents regarding congressional races in Florida and Pennsylvania (part of the larger batch given exclusively to The Hill); Pelosi denies that the documents came from her PC¹²

SEP 6

Guccifer 2.0 leaks alleged internal DCCC memo to the Observer; Observer publishes op-ed arguing that the memo reveals that the DCCC was cooperating with the Clinton campaign in 2015 – prior to Clinton becoming the Democratic nominee – and noted this to be a violation of the DCCC charter, which mandates impartiality towards all Democratic candidates¹³

SEP 13

Guccifer 2.0 leaks roughly 700 MB of alleged DNC data during the persona's "talk" at a London cybersecurity conference (the talk was delivered by a third party and read aloud from a script); data includes PII of top Obama White House officials and Virginia Senator/Democratic Vice Presidential Candidate Tim Kaine's personal cell phone number

SEP 15

Guccifer 2.0 leaks alleged DCCC research on districts and candidates, fundraising plans, and memos related to primaries in New Hampshire, Ohio, Illinois, and North Carolina

SEP 23

Guccifer 2.0 leaks alleged DCCC dossier on DCCC Chairman and New Mexico Congressman Ben Ray Lujan

OCT 4

Guccifer 2.0 leaks alleged documents from the Clinton Foundation; documents appear to actually have come from the DCCC

OCT 18

Guccifer 2.0 posts alleged DNC correspondence and documents discussing presidential candidate Donald Trump's finances, including copies of Trump's required Federal Election Commission (FEC) filings and plans to file Freedom of Information Act (FOIA) requests to discover additional information about the Republican candidate's finances

NOV 4

Guccifer 2.0 warns on Twitter and WordPress that "Democrats may rig the elections," and calls on hackers to monitor the elections for signs of fraud

NOV 6

WikiLeaks publishes approximately 8,000 additional alleged DNC emails that include discussions of the "Trump effect" and media interviews of persons of interest

2017**JAN 12**

Guccifer 2.0 posts a blog criticizing the "evidence" presented in the US Government's recently publicly released Russian hacking reports

⁹ https://twitter.com/GUCCIFER_2/status/756530278982684672

¹⁰ <http://thehill.com/policy/cybersecurity/291375-wordpress-blocks-latest-guccifer-20-docs>

¹¹ <http://thehill.com/policy/cybersecurity/292391-exclusive-guccifer-20-hacked-memos-expand-on-pennsylvania-house-races>

¹² <http://www.ibtimes.co.uk/nancy-pelosi-denies-pc-was-hacked-by-guccifer-2-0-still-blames-russia-1579738>

¹³ <http://observer.com/2016/09/new-guccifer-2-0-dccc-coordinated-with-clinton-campaign-in-2015/>

Section 1.2: DC Leaks



Period of Activity:
APRIL 2016 – OCTOBER 2016

Appropriated Brand:
WIKILEAKS

Websites:
ELECTIONLEAKS.COM, DCLEAKS.COM

Activity:
DATA LEAKS

Confidence in Russian State Sponsorship:
HIGH

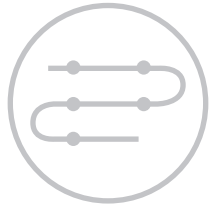
DC Leaks began leaking documents and email correspondence related to various then-current and former US Government officials and other individuals via the dcleaks.com site in June 2016, and continued to do so through October 2016. The persona claimed to be a project “launched by American hacktivists who respect and appreciate freedom of speech, human rights and government of the people” seeking to leak the email correspondence of “top ranking officials and their influence agents” in order to “find out and tell you the truth about U.S. decision-making process [sic] as well as about the key elements of American political life.” Despite leaking materials beginning in June, setup of the DC Leaks persona began as early as April 2016, with the registration of the domains dcleaks.com

and electionleaks.com. In a June 2016 email to a reporter at The Smoking Gun, the Guccifer 2.0 persona claimed that DC Leaks was a “sub-project” of anti-secrecy site WikiLeaks, however no such connection has been acknowledged by WikiLeaks.¹⁴ Although DC Leaks did not claim credit for the compromise of Clinton campaign chairman John Podesta’s email account (the contents of which were released by WikiLeaks), correspondence belonging to other individuals targeted as part of the same phishing campaign, attributed to Russian espionage group APT28 by Dell SecureWorks (see section 2.1), was published on the dcleaks.com website.¹⁵ This included correspondence allegedly belonging to former Secretary of State Colin Powell and Clinton campaign staffer William Rinehart.

¹⁴ <http://www.thesmokinggun.com/documents/investigation/tracking-russian-hackers-638295>

¹⁵ <https://www.secureworks.com/research/threat-group-4127-targets-hillary-clinton-presidential-campaign>

TIMELINE OF ACTIVITY



2016

APR 12

electionleaks.com
registered

APR 19

dcleaks.com registered

JUN 4

DC Leaks publishes correspondence allegedly belonging to military contractors, CENTCOM personnel, Republican Party employees, and campaign staffers for Senators John McCain, Lindsey Graham, and other individuals

JUN 7

DC Leaks releases documents including Clinton tax returns, memos, staffer biographies, and reports from the William J. Clinton Presidential Library; a Library spokesperson confirmed that the documents were publicly available via the Library's website¹⁶

JUN 8

Twitter account created; DC Leaks releases summaries of media reporting compiled by Hillary Clinton campaign staffers, and email correspondence belonging to Former NATO Commander and retired US General Philip Breedlove

JUL 13

DC Leaks publishes emails allegedly belonging to Clinton campaign staffer Sarah Hamilton

SEP 14

DC Leaks publishes emails allegedly belonging to former Secretary of State Gen. Colin Powell, including messages mentioning his views on presidential candidates Hillary Clinton and Donald Trump

SEP 22

DC Leaks publishes emails allegedly stolen from former White House and Clinton campaign staffer Ian Mellul

SEP 29

dcleaks.net registered. This domain was registered several months after DC Leaks had received mainstream attention; was not registered using the same registrar, DNS provider, AS provider, or email address as electionleaks.com and dcleaks.com (which shared these all in common); and appears to have never been used. As such, it is plausible the domain was not registered by the operators behind the DC Leaks persona but instead by a third party seeking to take advantage of the DC Leaks brand

SEP 30

DC Leaks posts password protected folders of data allegedly taken from State Department employee Sarah Stoll and Clinton campaign staffer Beanca Nicholson on Twitter and then gives Politico the password; Politico publishes an article on the leaks¹⁷

OCT 6

DC Leaks publishes emails allegedly belonging to former US Chief of Protocol Capricia Marshall, whom DC Leaks describes as a Clinton loyalist and Washington insider; DC Leaks also states that Marshall was named in allegations of campaign finance violations

OCT 7 - NOV 7

WikiLeaks publishes 34 separate batches of emails allegedly taken from John Podesta's Gmail account

OCT 19

DC Leaks provides the Daily Caller exclusive access to purported emails of White House staffer Zachary Leighton¹⁸

OCT 21

DC Leaks makes alleged emails of Sarah Stoll and Beanca Nicholson publicly available by removing the respective folders' password protections

OCT 31

DC Leaks makes purported emails of Zachary Leighton publicly available by removing the folder's password protection

¹⁶ <https://www.stripes.com/news/russian-hackers-of-dnc-said-to-scoop-up-secrets-from-nato-soros-1.423578>

¹⁷ <http://www.politico.com/story/2016/09/russia-hackers-clinton-campaign-state-department-228976>

¹⁸ <http://dailycaller.com/2016/10/19/exclusive-hundreds-of-white-house-staffers-emails-get-leaked/>

Section 1.3: @anpoland (Anonymous Poland)



Period of Activity:
JULY 2016 – NOVEMBER 2016

Appropriated Brand:
ANONYMOUS

Activity:
DATA LEAKS, DDOS, DEFACEMENTS

Known Open Source Tools:
SQLMAP, ACUNETIX, DIRBUSTER, HEIDISQL

Confidence in Russian State Sponsorship:
HIGH

@anpoland is a Twitter account purporting to represent “Anonymous Poland.” The account was first registered in 2010; however, except for one tweet that year and two retweets in 2012, the account appears to have been dormant until July 2016, when it threatened to conduct unspecified cyber threat activity in retaliation for threat activity claimed by the persona @pravsector that targeted Polish government and commercial entities (see section 1.5 below). The day following the threat, @anpoland claimed to have leaked five sets of data allegedly belonging to the Ukrainian Government and NATO, along with offensive statements and references to the controversial Ukrainian nationalist figure Stepan Bandera. The leaked documents appeared relatively mundane, and included, for instance, memos that appeared to have come from the Ukrainian Ministry of Foreign Affairs discussing cooperation with NATO and sets of statistics appearing to come from the Ukrainian Ministry of Internal Affairs.

From July 2016 to October 2016, @anpoland's activity meandered across three distinct categories: activity targeting Ukrainian and US Government and military entities, activity targeting organizations related to the 2016 Olympic games, and activity targeting the 2016 US elections. Analyzed collectively, @anpoland's behavior casts significant doubt on its claimed affiliation with Poland or the Anonymous collective, particularly given the persona's lack of ideological focus and the presence of substantial overlaps between @anpoland's activity and the behavior of the other personas discussed in this report (see sections 1.4, 2.3, and 3.2).

Most notably, after having previously leaked data from the Court of Arbitration for Sport in August 2016, it was @anpoland that first threatened to leak data from the World Anti-Doping Agency (WADA), tweeting on August 11: “Tomorrow will ddos WADA and publish some secret dosc [sic],” and then again on September 5: “within a few days will be new attack on the WADA/Olimpic [sic].” @anpoland did not articulate any clear motive for the threats, making only a series of vague comments on September 7 that included “I hate opimpic and sport [sic],” “I have sport and olimpic and now against everyone ... I hate ALL [sic],” and “pres.of WAda must be Kill. He like much money [sic].” However, the @anpoland account then went silent just prior to the Fancy Bears' Hack Team persona surfacing for the first time and claiming credit for the subsequent WADA leaks that allegedly occurred (see section 1.4). Furthermore, @anpoland's September 5 threat was issued the day before the @FancyBears Twitter account was registered. While at least one Polish athlete failed a drug test at the 2016 Rio Olympics, we did not observe any statements from @anpoland connecting the targeting of Olympic organizations to this athlete. The targeting of Olympics-related organizations represented a significant departure from the persona's initial anti-Ukraine and anti-NATO leaks and statements. As discussed in section 2.1, there is substantial evidence to suggest that the breach of WADA was conducted by the Russian cyber espionage group APT28.

Following the Fancy Bears' Hack Team persona's WADA leaks, @anpoland resurfaced in late October 2016 with a new focus on domestic US politics and the presidential election, leaking materials from the US-based conservative non-profit The Bradley Foundation, alongside claims that the documents demonstrated consort with Hillary Clinton's presidential campaign. Notably, @anpoland engaged in various manual and semi-automated dissemination tactics to promote the Bradley Foundation leak and related politicized narratives, including techniques we have termed "Direct Advocacy" and "Indirect Advocacy via Warlists" (see section 3.2 for a detailed discussion). The foray into anti-Clinton political messaging and the targeting of the Bradley Foundation represented yet another departure from the persona's prior anti-Ukrainian, and then anti-Olympic foci.

As with the Guccifer 2.0 persona and the "Pay to Play" episode discussed in section 1.1 above, we assess that some of the leaked documents purportedly associated with the Bradley Foundation were falsified by @anpoland to further encourage political narratives of a corrupt Clinton campaign. For example, on October 30, @anpoland promoted a screenshot of a purported letter from the Bradley Foundation to Rothschild Asset Management, Inc. that included the text

"Payment is required for Mrs Clinton's campaign. In this connection, we will withdraw \$150 million from the Rothschild portfolio on July 22th [sic]." Interestingly, allusions to a Clinton-Rothschild "global special interests" conspiracy appear to be a common theme promoted by suspected Russian and other troll networks on social media. In the promotional tweets, @anpoland included the comment "isn't a case of corruption? [sic]" and as part of its direct advocacy efforts, directed the tweets at various individuals including Trump campaign officials and the journalists John Pilger, Jake Tapper (CNN), Stefania Maurizi (La Repubblica), Ola Cichowlas (Moscow Times), Ian Wishart (Bloomberg), Duncan Robinson (Financial Times), Nikos Chrysoloras (Bloomberg), Ali Vitali (NBC News), Candace Smith (ABC), Bill O'Reilly (Fox News), Rebecca Ballhaus (Wall Street Journal), and George Stephanopoulos (ABC), in a seeming effort to have them pick up the story and further amplify the "corrupt Clinton" narrative. When asked about the letter, a Bradley Foundation representative denied its authenticity.¹⁹ Notwithstanding the ludicrously high \$150 million figure, which greatly exceeds campaign contribution limits, it is unlikely that the politically conservative Bradley Foundation would have made any monetary contributions to Hillary Clinton's presidential campaign.

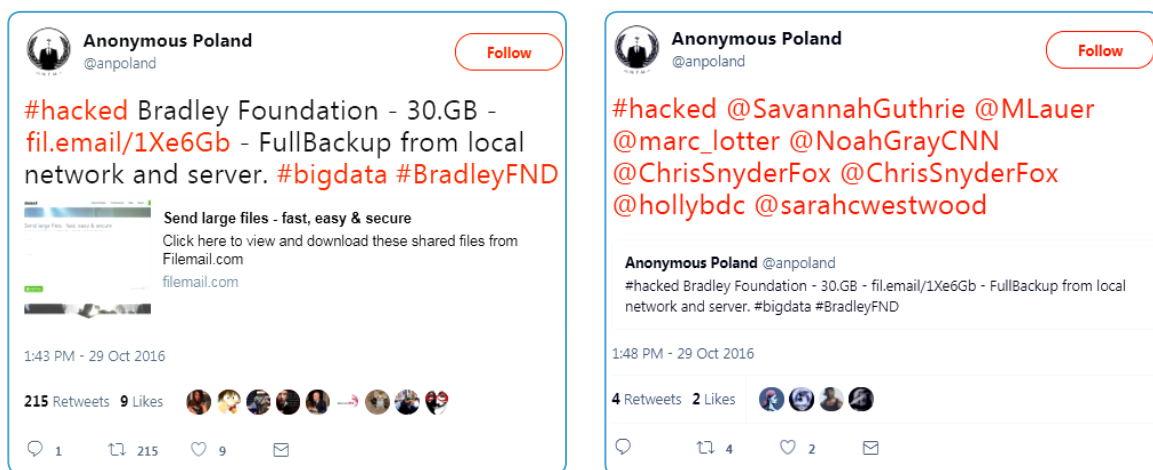


FIGURE 1.3.1: @ANPOLAND PUBLICIZES BRADLEY FOUNDATION LEAK AND ENGAGES IN "DIRECT ADVOCACY" ON TWITTER TO BRING THE LEAK TO THE ATTENTION OF SPECIFIC JOURNALISTS

¹⁹ <http://www.vocativ.com/372088/bradley-foundation-hack-clinton-campaign-fake-files/>

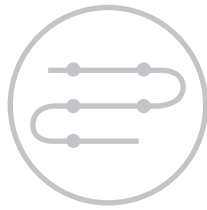


FIGURE 1.3.2: @ANPOLAND PERSONA PROMOTES A FALSIFIED EMAIL TO SPECIFIC INDIVIDUALS AS PART OF ITS “DIRECT ADVOCACY” EFFORTS

Despite @anpoland’s use of Anonymous imagery and slogans (such as #tangodown), and attempts to publicize leaks to other social media accounts known to disseminate hacktivist and Anonymous-related news (see section 3.2), with one exception, we did not observe genuine Polish or Anonymous-affiliated hacktivists endorsing or spreading @anpoland’s announcements. Based on our extensive observation and monitoring of historical Anonymous-affiliated campaigns and threat activity, this is unusual. The one exception regarding the alleged Bradley Foundation leak, was that the established Brazilian group

“Anonymous Globo” claimed via Twitter to have jointly conducted the operation with @anpoland. However, Anonymous Globo only began making these claims on November 1, three days after @anpoland originally announced the leak and began its concerted publicization campaign to promote it. We have observed no additional evidence of Anonymous Globo’s involvement with the Bradley Foundation compromise and judge that the group retroactively picked up on @anpoland’s announcements and falsely claimed involvement, likely as a means of boosting its own reputation.

TIMELINE OF ACTIVITY



2016

JUL 29

@anpoland directs a tweet at "@pravsector," a suspected false hacktivist persona claiming Ukrainian affiliation. In the tweet, @anpoland threatens to conduct unspecified cyber threat activity in reaction to previous @pravsector activity targeting Polish government and commercial entities

AUG 1

@anpoland claims to have leaked five sets of data allegedly belonging to the Ukrainian Government and NATO. The documents appear to be relatively mundane, including memos that appear to come from the Ukrainian Ministry of Foreign Affairs discussing cooperation with NATO, and sets of statistics that appear to come from the Ukrainian Ministry of Internal Affairs

AUG 10

@anpoland claims to leak data from the CAS, the Detroit Police Department, and data allegedly related to the Boeing KC-10 aircraft and the US Air Force Strategic Air Command. In a video, @anpoland displays the websites of CAS and WADA, both of which appear to have been defaced with news article headlines stating, "WE FORGOT THE SPORT IS OUT OF THE POLITIC. PLEASE FORGIVE US [sic];" we were unable to independently corroborate these claimed defacements

AUG 10-11

The "USA News" Warlist (see section 3.2) promotes @anpoland's claimed leaks of data from the US Strategic Air Command Boeing, and CAS, as well as @anpoland's claim of a DDoS attack against CAS

AUG 11

@anpoland claims to have conducted a DDoS attack against the CAS website. We observed that the CAS website was unavailable immediately following the claim, indicating that the website had indeed been disabled

@anpoland also threatens to conduct a DDoS attack against, and to leak data from, WADA

SEP 5

@anpoland again threatens to release data purportedly stolen from WADA

SEP 7

@anpoland releases two videos that depict claimed defacements of the official websites of the International Paralympic Committee (paralympic.org) and the US Olympic Committee (teamusa.org). There is some very limited evidence, namely third-party observation on social media, that @anpoland successfully defaced both websites, though it is also plausible that the defacements were falsified

OCT 29

@anpoland claims to have leaked data from the Bradley Foundation; one of the leak announcements also contains the hashtag #HillaryDown, which is subsequently amplified through Warlist activity (see Section 3.2)

OCT 29-NOV. 1

"Anti-Global" Warlist promotes the Bradley Foundation Leak

NOV 2-3

"ClintonCorruption" Warlist promotes the Bradley Foundation leak

NOV 3

@anpoland claims to have conducted a DDoS attack against the Bradley Foundation

"ClintonCorruption [sic]" Warlist promotes the Bradley Foundation DDoS attack

NOV 8

US election day; @anpoland tweets messages expressing opposition to the Democratic Party and Hillary Clinton that include the hashtag #WarAgainstDemocrats." Subsequently, "Russian Prostitute" and "GOP - WAR" Warlists attempt to trend the #WarAgainstDemocrats hashtag

NOV 9

"Russian Prostitute" and "GOP - WAR" Warlists merge to become the "GOP - WON" Warlist, celebrate Bradley Foundation leak and Clinton electoral loss

Section 1.4: Fancy Bears' Hack Team



Period of Activity:
SEPTEMBER 2016 - PRESENT

Appropriated Brands:
ANONYMOUS, FANCY BEAR

Websites:
FANCYBEAR.NET, FANCYBEAR.ORG

Activity:
DATA LEAKS

Confidence in Russian State Sponsorship:
HIGH

The persona Fancy Bears' Hack Team, which portrays itself as an Anonymous-affiliated hacktivist group, first surfaced and started claiming to leak sets of athlete medical data allegedly stolen from the World Anti-Doping Agency (WADA) in September 2016. The persona leaked various athletes' purported Therapeutic Use Exemptions (TUEs), documents that authorized named athletes to use otherwise banned substances for legitimate medical purposes. The releases of the TUEs, which spanned September and early October, were accompanied by politicized narratives from Fancy Bears' Hack Team and pro-Russia social media accounts suggesting that a corrupt WADA was actively facilitating illegal doping by athletes from some countries, despite having banned Russian athletes from the 2016 Olympics and Paralympics for the same behavior (see Figure 1.4.1). Permitted, disclosed, and authorized medicinal use by athletes was implied to be equivalent to the Russian state-sponsored scheme to provide illegal substances to athletes and falsify drug test records. In Fancy Bears' Hack Team's December 2016 announcement accompanying a claimed leak of email correspondence between the US Anti-Doping Agency (USADA) and the Canadian Center for Ethics in Sport (CCES), the persona claimed that the US and Canadian agencies were primarily concerned with furthering the political interests of their countries, not clean sport (see Figure 1.4.2). Significantly, this theme echoes the @anpoland persona's August 10, 2016 claimed defacements of the websites of WADA and the Court of Arbitration for Sport (CAS), which featured the language, "WE FORGOT THE SPORT IS OUT OF THE POLITIC. PLEASE FORGIVE US [sic]."

On Sept. 13, 2016, WADA publicly confirmed that the Russian cyber espionage group FireEye tracks as APT28 had gained unauthorized access to its Anti-Doping Administration and Management System (ADAMS) database between August 25, 2016 and September 12, 2016 using credentials compromised via phishing, and that the first

set of materials leaked by the Fancy Bears' Hack Team persona included legitimate confidential medical data.²⁰ In November 2016, WADA officials disclosed that 18 of the 228 TUEs released by Fancy Bears' Hack Team had been falsified.²¹ The officials did not elaborate as to the nature of the falsifications, but open source reporting indicates one case in which a TUE for a Dutch cyclist had been altered with images of official stamps to make it appear to apply to the Rio 2016 Olympics, while much of the content in the alleged TUE actually appeared in a legitimate TUE for a 2008 event.²² Between November 2016 and at least March 2017, Fancy Bears' Hack Team engaged in direct, private communications with journalists, including offering privileged access to leaked materials, in an attempt to encourage journalists to cover the leaks (see Figure 1.4.3, section 3.2).



FIGURE 1.4.1: FANCY BEARS' HACK TEAM PROMOTES THE NARRATIVE THAT WADA ENFORCEMENT ACTION AGAINST RUSSIAN ATHLETES IS HYPOCRITICAL

²⁰ <https://www.wada-ama.org/en/media/news/2016-09/wada-confirms-attack-by-russian-cyber-espionage-group>;
<https://www.wada-ama.org/en/media/news/2016-10/cyber-security-update-wadas-incident-response>

²¹ <http://news.nationalpost.com/sports/olympics/wada-claims-russian-hackers-leaked-fake-medical-records-in-effort-to-discredit-legitimate-use-of-banned-drugs>

²² <http://www.cyclingnews.com/news/cancellara-cummings-fuglsang-featured-in-latest-fancy-bears-leak/>

We assess with high confidence that the Fancy Bears' Hack Team persona was a direct continuation of the Olympics-related threat activity first conducted by @anpoland, and that the operator(s) behind these personas are either one and the same or very closely affiliated. As noted in section 1.3, @anpoland twice threatened to leak data specifically from WADA, but failed to follow through on that threat. Both personas used strikingly similar tactics for publicizing their activity, particularly direct, rapid notifications to international journalists and social media accounts known to disseminate hacktivist and information security news (see section 3.2). "Fancy Bear" is the name cyber security firm CrowdStrike uses to describe the set of Russia-nexus cyber espionage activity FireEye tracks as APT28. The incorporation of this name into the purported hacktivist persona appears to have been a deliberate attempt to create further confusion regarding the accurate attribution of cyber threat activity, and perhaps even to mock security researchers regarding then-recent high-profile public attributions to Russia. The Fancy Bears' Hack Team persona surfaced during a period of heightened media attention surrounding APT28-attributed cyber activity targeting the 2016 US elections.

Additionally, similar to the @anpoland persona's activity, despite Fancy Bears' Hack Team's use of Anonymous imagery and language, and its similar attempts to publicize leaks to disseminators of hacktivist and Anonymous-related news, immediately following the persona's first leak announcements we observed only nominal instances of other Anonymous-affiliated hacktivists endorsing or propagating news of the activity. Once again, this limited promotion was highly inconsistent with our extensive historical observation and analysis of Anonymous-affiliated hacktivist activity.



FIGURE 1.4.2: FANCY BEARS' HACK TEAM CLAIMS THAT USADA AND CCES ARE POLITICALLY MOTIVATED

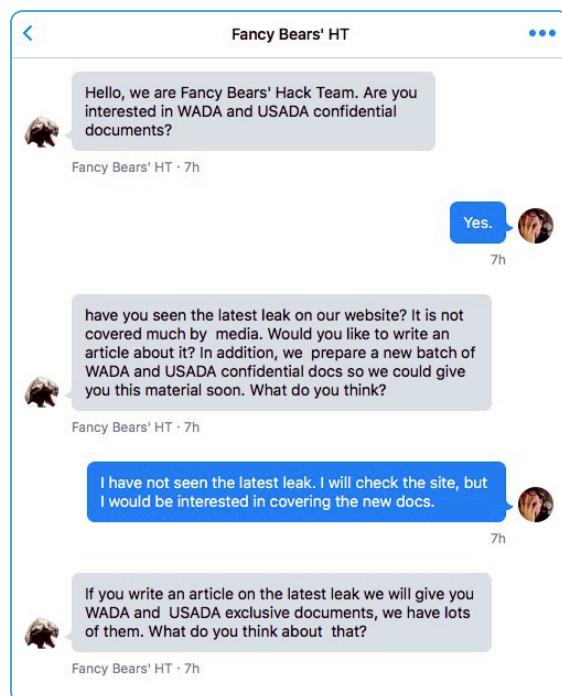


FIGURE 1.4.3: SCREENSHOT OF TWITTER DIRECT MESSAGES BETWEEN FANCY BEARS' HACK TEAM AND ARS TECHNICA REPORTER SEAN GALLAGHER²³

²³ <http://arstechnica.com/security/2016/12/hackers-behind-anti-doping-leaks-please-write-about-us-well-give-you-exclusive/>

TIMELINE OF ACTIVITY

2016
SEP 1

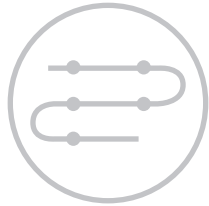
The domains fancybear.net and fancybear.org are registered

SEP 6

@FancyBears Twitter account created

SEP 12

Fancy Bears' Hack Team leaks alleged confidential TUEs belonging to prominent US athletes from WADA


SEP 12

@FancyBearsHT Twitter account created

SEP 12

An unnamed Warlist promotes WADA leak by Fancy Bears' Hack Team

SEP 14

Fancy Bears' Hack Team leaks second set of alleged athlete TUEs from WADA

SEP 16

Fancy Bears' Hack Team leaks third set of alleged TUEs from WADA

SEP 19

Fancy Bears' Hack Team leaks fourth set of alleged TUEs from WADA

SEP 23

Fancy Bears' Hack Team leaks fifth set of alleged TUEs from WADA

OCT 3

Fancy Bears' Hack Team leaks sixth set of alleged TUEs from WADA

OCT 6

Fancy Bears' Hack Team claims to leak emails from USADA

DEC 13

Fancy Bears' Hack Team claims to leak additional emails from USADA and the Canadian Center for Ethics in Sport (CCES) that allegedly demonstrate that the US and Canada conspired against the International Olympic Committee (IOC) "to further their political interests."

DEC 16

Fancy Bears' Hack Team actively solicits reporters to cover their leak activity, including one at Ars Technica²⁴

2017
JAN 15

Der Spiegel publishes an article discussing anti-doping efforts based on WADA and USADA materials purportedly stolen and provided exclusively to the publication by Fancy Bears' Hack Team²⁵

JAN 18

Fancy Bears' Hack Team promotes Der Spiegel article via Twitter

JAN 26

Fancy Bears' Hack Team publishes a Tweet calling attention to a BBC article that referenced leaked TUEs²⁶

FEB 26

The Sunday Times publishes an article about doping allegations related to a track and field training program and associated athletes based on alleged USADA documents stolen by "Fancy Bears"²⁷

MAR 4

Der Spiegel publishes an article discussing doping allegations related to a track and field training program based on the same alleged USADA documents referenced in The Sunday Times article²⁸

MAR 6

Fancy Bears' Hack Team publishes Tweets referencing The Sunday Times and Der Spiegel, likely to call attention to the articles and to allegations of athlete "doping"

MAR 17

March 17 - Der Spiegel publishes an article discussing doping allegations of soccer players based on an alleged "WADA spreadsheet" provided to the publication by Fancy Bears' Hack Team²⁹

MAY 19

The New York Times publishes an article discussing doping allegations related to a track and field training program documented in a report Fancy Bears' Hack Team claims to have stolen from USADA³⁰

MAY 23

Fancy Bears' Hack Team publishes tweets referencing the May 19, 2017 New York Times article discussing the allegedly leaked USADA report about a track and field training program as well as an April 20, 2017 BBC article discussing doping allegations for a British cyclist³¹

JUL 5

Fancy Bears' Hack Team claims to leak emails from WADA and the International Association of Athletics Federations (IAAF)

²⁴ <http://arstechnica.com/security/2016/12/hackers-behind-anti-doping-leaks-please-write-about-us-well-give-you-exclusive/>

²⁵ <http://www.spiegel.de/international/world/sports-doping-and-the-difficult-fight-to-prevent-it-a-1129918.html>

²⁶ <http://www.bbc.com/sport/cycling/38728410>

²⁷ <http://www.thetimes.co.uk/article/leaked-doping-report-says-mo-was-given-risky-treatment-65nxsvmhs>

²⁸ <http://www.spiegel.de/sport/sonst/nike-oregon-project-usada-erhebt-schwere-vorwuerfe-gegenweltklasselaeufer->

²⁹ <http://www.spiegel.de/international/zeitgeist/football-rife-with-performance-enhancing-drugs-a-1139238.html>

³⁰ <https://www.nytimes.com/2017/05/19/sports/nike-oregon-project-alberto-salazar-dathan-ritzenhein.html>

³¹ <http://www.bbc.com/sport/cycling/39654790>

Section 1.5: @pravsector



Period of Activity:
JULY 2016 – AUGUST 2016

Appropriated Brand:
RIGHT SECTOR (UKRAINIAN NATIONALIST
MILITIA AND POLITICAL GROUP)

Activity:
DATA LEAKS

Known Open Source Tools:
P.A.S. SHELL

Confidence in Russian State Sponsorship:
HIGH

In July 2016, the operator(s) behind Twitter accounts @pravsektor and @pravysektor, professing affiliation with the Ukrainian ultranationalist (and anti-Russian) paramilitary group "Right Sector" (Ukrainian: Правий Сектор; transliterated: Pravyi Sektor), claimed to have leaked data from the Polish telecommunications company Netia and the Polish Ministry of Defense (MOD), including data purportedly regarding the US PRISM surveillance program. Netia confirmed that unknown perpetrators had stolen data from its website's backend databases,³² and we judge, and a Polish MOD spokesperson confirmed, that @pravsektor gained access to at least one computer or email account belonging to a Polish MOD employee, but exaggerated the level of access obtained and the sensitivity and significance of the leaked data.³³ We believe that the alleged US PRISM "logs" were falsified, with the logs appearing to have been generated by credential collection malware. As noted in section 1.3, this initial @pravsektor activity was the purported impetus for the @anpoland persona's emergence and early activity targeting the Ukrainian Government and NATO (see Figures 1.5.1, 1.5.2). The @pravysektor Twitter account was registered on June 1 or 2, 2016, and the @pravsektor account was registered in early July 2016. Both accounts are now suspended. As the @pravsektor account was the most active, we use that throughout this report as the persona's namesake.

The timing and targets of @pravsektor leaks, as well as the commentary that accompanied them, appeared to be intended to undermine relationships between Poland and NATO, Poland and the US, Poland and Ukraine, and between Right Sector supporters and other Ukrainians. For example, @pravsektor statements indicate that the motivation for the Netia leak was a resolution passed by the Polish Senate urging the lower house of Parliament to recognize the 1943-44 massacres of ethnic Polish people in

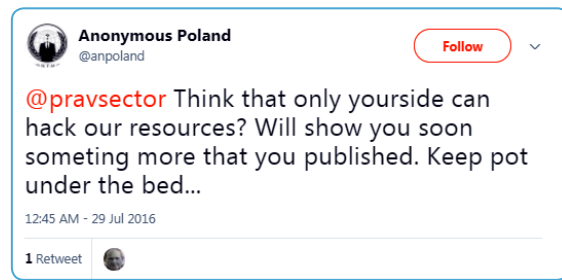


FIGURE 1.5.1: @ANPOLAND REACTS TO @PRAVSEKTOR ACTIVITY



FIGURE 1.5.2: @PRAVSEKTOR RESPONDS TO @ANPOLAND THREAT

Nazi-occupied Poland by Ukrainian nationalists as genocide, and to establish a National Day of Remembrance for the victims on July 11. We believe that @pravsektor's references to the Volhynia and Eastern Galicia massacres, suggestions that the modern day Right Sector group is linked to the Ukrainian nationalist militia that carried out these killings, and use of anti-Polish slurs were intended to stir up historical animosities between Ukraine and Poland immediately preceding the July 2016 NATO summit in Warsaw, which began on July 8, 2016. These statements, as well as racial slurs directed at Ukrainians of Armenian descent, also serve to damage the reputation of the Right Sector organization.

³² <http://www.ibtimes.co.uk/netia-data-leak-polish-telco-operator-hacked-14gb-customer-credentials-posted-online-1570051>

³³ <https://www.defensenews.com/2016/07/15/ukrainian-nationalists-claim-cyberattack-on-polish-defense-ministry/>

Similarly, we believe that @pravsector statements and altered materials alleging links between the Polish MOD and the US PRISM surveillance program were intended to incite suspicion regarding alleged US surveillance of Europeans. Accusations of biological testing, we suspect, were intended to cast US support for Ukraine in its conflict against pro-Russian separatists in a negative light. Later commentary from @pravsector about the DNC compromise and Guccifer 2.0 leaks represented a notable departure from the persona's early focus on the relationship between Poland and Ukraine (see Figure 1.5.3).

While some of the persona's political messaging appears to be consistent with Right Sector ideology, the strong anti-Polish sentiment expressed by @pravsector does not appear to be shared by Right Sector (see Figure 1.5.4). Indeed, a Right Sector spokesman reportedly publicly denied any connection between the organization and the @pravsector persona, claiming that the persona was fake, though this itself does not preclude such a connection.³⁴ The fact that the two Twitter accounts associated with the persona, @pravysektor and @pravsector, were created in June and July 2016 respectively (almost immediately prior to the leaks), and therefore possessed very little history involving the Right Sector and its political activities, further casts doubt over the accounts being legitimately affiliated with the genuine Right Sector organization (the @pravysektor account did retweet content from authentic Right Sector accounts from its creation in early June until the attack claims in July).

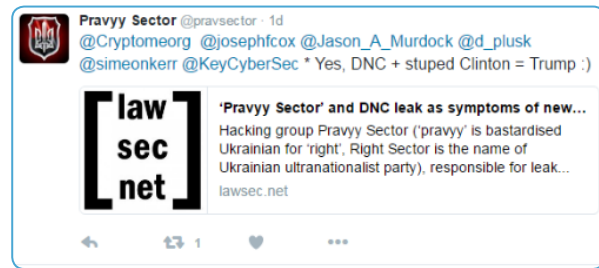


FIGURE 1.5.3: @PRAVSECTOR REFERENCES POLISH BLOG POST COMPARING DNC LEAK TO @PRAVSECTOR ACTIVITY³⁴

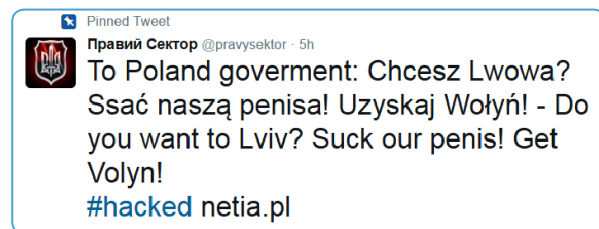
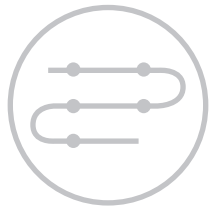


FIGURE 1.5.4: @PRAVYSEKTOR ACCOUNT ANNOUNCES NETIA BREACH ON JULY 7

³⁴ <https://lawsec.net/2016/08/01/pravvy-sector-and-dnc-leak-as-symptoms-of-new-trend-in-russian-cyber-operations/>

³⁵ <http://in.reuters.com/article/poland-netia-cybercrime-idINKCN0ZQ23H>

TIMELINE OF ACTIVITY



2016

JUN 1 OR 2

@pravysektor Twitter account registered

JUL 1-7

@pravysektor Twitter account registered

JUL 7

The @pravysektor account claims to leak approximately 14 GB of data from Polish telecommunications company Netia. Leaked data includes customer PII and employee login credentials.

@pravysektor statements include disparaging references to the Polish Senate's vote to recognize the Volhynia and Galicia massacres as genocide, and other offensive and racially charged language

JUL 7

"Poland News" Warlist promotes Netia data leak

JUL 14-15

@pravysektor claims to have leaked data from the Polish Ministry of Defense (MOD) and makes statements referencing the US PRISM surveillance program that imply a connection between the MOD and US surveillance activities. @pravysektor also threatens to release additional information from the MOD if the Polish Government does not pay a ransom of \$50,000 US. We doubt that the extortion attempt was intended to generate profit for the group; rather we believe that the extortion claim, and the use of a famous Right Sector member's bitcoin wallet were intended to call additional attention to the leak

JUL 18

@pravysektor claims to leak data from German investment firm Gap Vermögensverwaltung GmbH along with the words "Hello, Frau Merkel !" The leaked data primarily consists of Excel spreadsheets, Word documents, and email messages, as well as JPEG and PDF files. GAP customer PII, PII of GAP employees, and plaintext employee usernames and passwords are also included in the leak

JUL 21

@pravysektor claims to leak login credentials for the Ukrainian Ministry of Foreign Affairs website, emails belonging to the Ukrainian Minister of Internal Affairs Arsen Avakov, and data from the Armenian Embassy in Ukraine, accompanied with the words "@Fuck #Armenia #Fuck #Avakov." Minister Avakov is of Armenian descent

JUL 21-AUG 1

"Ukraine.info" Warlist promotes Armenian Embassy data leak

AUG 1

@pravysektor leaks data purportedly stolen from the Central Ohio Urology Group, claiming that it demonstrates the "Pentagon conducted bacteriological [sic] tests in Ukraine." @pravysektor also posts links to an InfoWars article alleging that the US military is testing biological weapons at laboratories in Ukraine, and a screenshot that appears to demonstrate the persona's unauthorized access to the Ohio Urology Clinic. @pravysektor labeled the screenshot "hacked mil pc" to suggest that the clinic was somehow connected to the military

AUG 1-2

"IT News" Warlist promotes @pravysektor messaging

AUG 2

"China Daily" and "EuroPress" Warlists promote @pravysektor messaging

AUG 2

@pravysektor tweets a link to a Polish blog article comparing the Netia and Polish MOD breaches to the DNC breach, accompanied by the words "Yes, DNC + stuped [sic] Clinton = Trump"³⁶

³⁶ <https://lawsec.net/2016/08/01/pravy-sector-and-dnc-leak-as-symptoms-of-new-trend-in-russian-cyber-operations/>

Section 1.6: Bozkurt Hackers (aka Hacker Buba)



Period of Activity:
NOVEMBER 2015 – AUGUST 2016

Appropriated Brand:
GREY WOLVES (TURKISH NATIONALIST MILITIA
AND POLITICAL GROUP)

Activity:
DATA LEAKS

Known Open Source Tools:
SQLMAP, JSP FILE BROWSER, HAVIJ, P.A.S. SHELL, AJS SHELL

Confidence in Russian State Sponsorship:
MODERATE

In November 2015, the actor “Hacker Buba” claimed to leak SQL and Excel files containing account holder and credit card transaction data, from UAE based InvestBank, following a failed extortion attempt. The chief financial and operations officer of InvestBank confirmed that Hacker Buba had communicated with representatives of InvestBank and threatened to publish sensitive customer financial data if the bank did not pay a ransom, but stated “We won’t give in to any extortion threat.”³⁷ Media sources reported that the demanded ransom amount was approximately \$3 million USD to be denominated in bitcoin.³⁸ In March 2016, an actor using the handle “bozkurt.3754” posted messages to an underground forum claiming that Hacker Buba had been killed, and that he had requested that additional data purportedly taken from InvestBank be released “if with him something will happen [sic].” Subsequently, in April 2016, Bozkurt Hackers leaked alleged

account and transaction data from Qatar National Bank (QNB). The persona operators created folders among the leaked files to call attention to data allegedly belonging to employees of Al Jazeera, members of the Qatari royal family, the family of Yusuf Al-Qaradawi (an Egyptian scholar with ties to the Muslim Brotherhood), as well as folders for “gov,” defense, intelligence, police, and other individuals that the attackers identified as being “spies.” In May 2016, the Bozkurt Hackers persona claimed to have leaked data from Nepalese banks Business Universal Development Bank (data apparently stolen from an email server), and Sanima Bank (account and transaction information); Bangladeshi banks Dutch-Bangla Bank (ATM transaction information, employee logins), The City Bank (customer PII), Trust Bank (employee login credentials); and Sri Lankan bank the Commercial Bank of Ceylon (employee logins).

³⁷ <https://www.wired.com/2015/12/hacker-leaks-customer-data-after-a-united-arab-emirates-bank-fails-to-pay-ransom/>

³⁸ <https://www.dailydot.com/layer8/invest-bank-hacker-buba/>

The Bozkurt Hackers persona presented itself as affiliated with the Turkish nationalist political group and militia known as the Grey Wolves (aka Bozkurtlar). The Grey Wolves are a right-wing Turkish nationalist youth organization associated with the Nationalist Movement Party (MHP). Critics accuse the MHP and the Grey Wolves of being "neo-fascist" and intolerant of minority groups, including the Kurds; the Grey Wolves have also been described by some critics as a quasi-state-sponsored ethno-nationalist militia and a terrorist organization. However, we judge that the Bozkurt Hackers persona's behavior was inconsistent with this claimed affiliation. For example, only one of the eight Bozkurt Hackers leaks, that from QNB, was accompanied by any clear political messaging, which in that case attempted to call negative attention to the Qatari royal family, Qatari security institutions, Al Jazeera, and the presence of Egyptian Muslim Brotherhood scholar Yusuf Al-Qaradawi in Qatar.

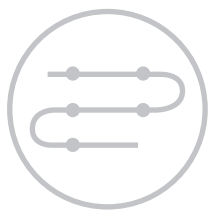
The attempt to portray these groups and institutions negatively contrasted sharply with Turkish interests and that country's collaborative relationship with Qatar, at a time when military and political cooperation between the two nations was strong in several arenas, perhaps most prominently regarding the Syrian conflict, where Qatar and Turkey were both supporting Syrian fighters opposing the regime of Bashar al-Assad. Notably, Grey Wolves fighters were reported to be defending ethnic Turkmen Syrians against Assad regime and Russian military offensives, and a Grey Wolves fighter was reportedly responsible for killing the pilot of a Russian fighter jet that was shot down by Turkey in November 2015 along its southern border with Syria. A photo posted on Facebook we observed that generated Russian-language media attention suggests that Grey Wolves members also traveled to the border area between Crimea and Ukraine's Kherson Oblast to visit prominent members of the Crimean Tatar community, to the apparent consternation of commentators in Russia.³⁹

If Bozkurt Hackers were genuinely sympathetic to – and motivated by – Grey Wolves ideology, we would have expected to see clear and consistent political statements to that effect, statements closely aligned with Turkish national interests. Likewise, we would have expected to see the group target entities associated with Turkish adversaries rather than entities in the Arabian Peninsula and South Asia, such as those associated with Kurdish militias and organizations, or targets in Russia, Armenia, or China, where the Grey Wolves seek to support ethnic Turkic diaspora communities. We also observed no evidence to indicate that Bozkurt Hackers was endorsed by or associated with any of the genuine hacktivist actors and groups that do appear to support the Grey Wolves, such as "Bozkurt Hacker Tim," "Bozkurt Siber Tim," "BoZKuRTSeRDaR," and "Wolf Team Bozkurt Hackers."

We are also highly skeptical that Bozkurt Hackers' activity was financially motivated. It is unusual for financially motivated actors to seek to draw excessive public attention to their activity in the manner that Bozkurt Hackers did (see section 3.2), and the public release of compromised data also undermines the potential to directly profit from it. The persona leaked data from seven of its eight known victims within a single six-day period in early May 2016, and evidence in the leaked data suggests that, for five of these victims, at least five months had passed since the attackers had last had access to victim systems. If the primary goal of Bozkurt Hackers had been extortion, we would expect the releases, which presumably would have followed failed extortion attempts, to have occurred independently of one another, and likely while Bozkurt Hackers either still had access to victim systems or soon after they had lost access. We also did not observe any evidence of the sale or exploitation of data allegedly stolen from the eight banks Bozkurt Hackers targeted, though it is plausible that monetization could have occurred in private. Instead, we observed a small number of posts on underground forums advertising the QNB and InvestBank data for free, again casting doubt on the activity having been financially motivated.

³⁹ <https://sputniknews.com/analysis/201512101031518376-grey-wolves-threat-to-crimea/>

TIMELINE OF ACTIVITY


2015
NOV 17

Hacker Buba begins publishing individual tweets containing alleged account data belonging to InvestBank customers

DEC 3

Hacker Buba posts a download link to approximately 250MB of purported InvestBank account data to Twitter, claiming to have previously attempted to extort InvestBank

2016
MAR 26

A "guest" user posts a link to a Google Drive hosting additional alleged InvestBank account holder data to Pastebin⁴⁰

MAR 28

The user "bozkurt.3754" posts a link to the same Google Drive hosting alleged InvestBank account holder data to a cybercrime forum

APR 20

Bozkurt Hackers leaks alleged account and transaction data from Qatar National Bank (QNB) using several Twitter accounts using variations on the name "Anti QNB" (for example @q_n_b1)

APR 20

"QNB" Warlist begins promoting Bozkurt Hackers activity

MAY 6

Bozkurt Hackers leaks additional alleged InvestBank account data

MAY 9

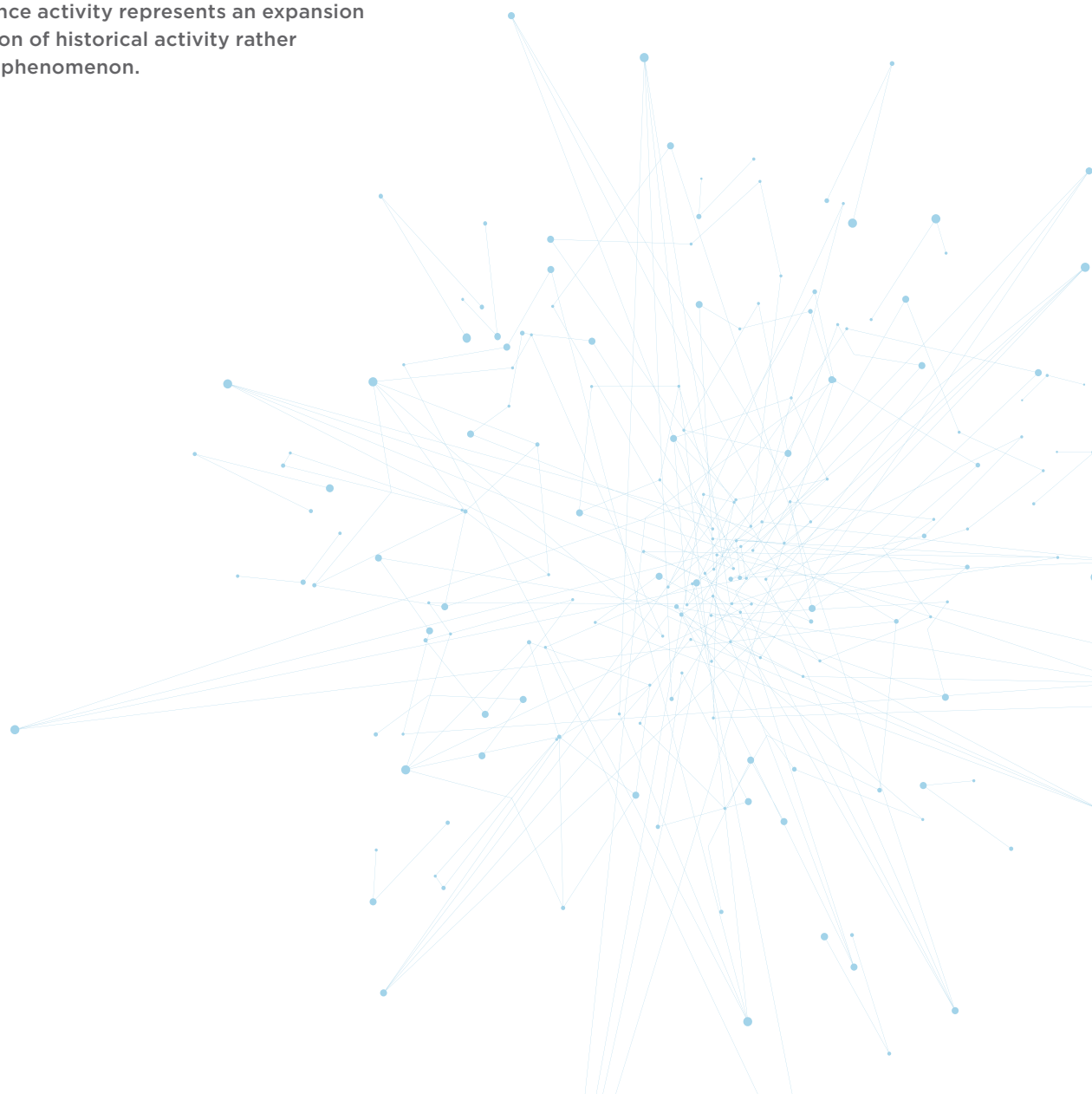
Bozkurt Hackers claims to leak data from Nepalese banks Business Universal Development Bank (data apparently stolen from an email server) and Sanima Bank (account and transaction information); Bangladeshi banks Dutch-Bangla Bank (ATM transaction information, employee logins), The City Bank (customer PII), Trust Bank (employee login credentials); and Sri Lankan bank the Commercial Bank of Ceylon (employee logins)

⁴⁰ <https://pastebin.com/p8pEiUct>

1.7: Other Personas

Assessment 2

The six preceding false hacktivist personas discussed are not the only hacktivist personas we believe Russia has leveraged in support of information operations. We have previously assessed, with differing respective degrees of confidence, that the “CyberCaliphate” and “CyberBerkut” hacktivist personas were deployed to support influence campaigns beginning in 2014. As such, we assess Russia’s 2016 influence activity represents an expansion and evolution of historical activity rather than a new phenomenon.



1.7.1: CyberCaliphate



Period of Activity:
DECEMBER 2014 – AUGUST 2015

Appropriated Brand:
ISIS

Website:
CYB3RC.COM

Activity:
DATA LEAKS, CREDENTIAL COMPROMISES, DEFACEMENTS,
DATA DESTRUCTION

Confidence in Russian State Sponsorship:
HIGH

CyberCaliphate, which portrayed itself as a pro-Islamic State (ISIS) hacktivist group, was active from December 2014 to August 2015. The persona conducted a series of high-profile defacements and compromises against media organizations and US Government targets. CyberCaliphate is best known for its April 2015 destructive attack against French television station TV5Monde, an incident that demonstrated a much higher level of sophistication than any threat activity we had observed from any other purported pro-ISIS hacktivist – including previous CyberCaliphate compromises. Our attribution of Russian sponsorship stems from the presence of an active infection of proprietary APT28 malware CORESHELL at TV5Monde in February 2015, confirmations from French investigators and TV5Monde that APT28 was the probable culprit behind the April 2015 CyberCaliphate attack,⁴¹ similarities in domain registration activity by APT28, and the registration for the CyberCaliphate website cyb3rc.com.

There has been persistent confusion about the term “cyber caliphate” due, in part, to media reporting and other commentary that has conflated and sensationalized sets of activity, groups, and/or general trends among Internet users potentially sympathetic to Islamist extremist ideologies, or Internet users simply perceived to be linked to extremism. The confusion about the term has been further perpetuated by both the Russian-sponsored false hacktivist persona CyberCaliphate itself, and by genuine pro-ISIS hacktivists seeking

to appear more threatening or prominent than they actually are by claiming credit for activity conducted by CyberCaliphate.

The term “cyber caliphate” may have originated in 2012 English language media reports describing Muslim Brotherhood figure Tareq Al-Suwaïdan as encouraging the creation of a caliphate and perpetration of “cyber jihad” hacktivist activity directed against the state of Israel.⁴² It is important to note that al-Suwaïdan is not affiliated with the Islamic State (ISIS) or Al-Qa’ida (AQ). We also observed other English language online commentary in 2012 using the term “cyber caliphate” as a general term to describe Muslim online activity that authors perceived as undesirable.⁴³

In the fall of 2014, media reporting claimed that ISIS and/or Al-Qa’ida affiliated actors were seeking to establish a “cyber caliphate.”⁴⁴ However, we believe that this media reporting conflated several disparate entities and incidents, including now defunct hacktivist group the Tunisian Cyber Army, the emergence of other hacktivist groups incorporating the names of ISIS and AQ, aspirational statements regarding jihadist cyber threat capabilities by individuals such as former Al-Qa’ida in Iraq (AQI) leader Abu Hamza al-Muhajir (deceased in 2010) that do not reflect capabilities or resource allocations, and use of anonymizing techniques such as encryption, virtual private networks (VPNs), and The Onion Router (TOR) network by ISIS and AQ members and supporters.

⁴¹ <http://www.bbc.com/news/technology-37590375>

⁴² <https://www.memri.org/reports/kuwaiti-muslim-brotherhood-leader-and-director-saudi-al-ri-sala-tv-tareq-al-suwaïdan-tours>

⁴³ <http://mideastposts.com/middle-east-society/harun-yahya-abusing-islam-to-spread-creationist-myth/>

⁴⁴ <http://www.foxnews.com/world/2014/09/14/digital-jihad-isis-al-qaeda-see-cyber-caliphate-to-launch-attacks-on-us.html>

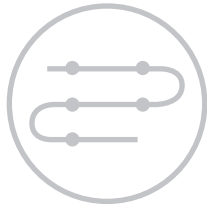
The CyberCaliphate persona, claiming to be motivated by a pro-ISIS ideology, first emerged in December 2014 and was active through April 2015, with a limited re-emergence in August 2015. We consider the activity claimed by CyberCaliphate during this timeframe to be a unified set of activity likely conducted by a single set of operators based on distinct TTPs, targeting, messaging, iconography, and links to the domain cyb3rc.com. We did not observe any other hacktivist actors or supporters, pro-ISIS or otherwise, claim the moniker "CyberCaliphate" from December 2014 to August 2015, though the number of pro-ISIS hacktivist actors and groups expanded markedly between the latter half of 2014 and the Fall of 2015, at which time the growth of new groups subsequently slowed.

In September 2015, the pro-ISIS hacktivist group "Islamic Cyber Army" (ICA) surfaced. One member of this group adopted the moniker "CyberCaliphate," likely in an effort to claim credit for or otherwise associate with the high-profile activity conducted by the false hacktivist persona of the same name. We believe that the ICA deliberately uses multiple names, many of which incorporate the terms "cyber" and "caliphate," including "Caliphate Cyber Army" (CCA) and "United Cyber Caliphate" (UCC), frequently calls for other pro-ISIS hacktivist groups to unite under its banner, and regularly announces mergers and name changes. We believe that these naming conventions and calls for consolidation are intended to make the group appear larger and more prominent than it is, and to claim credit for cyber threat activity conducted by other actors. We have observed

no evidence to support the hypothesis that there is a connection between the false hacktivist persona "CyberCaliphate," which was active from December 2014 to April 2015, and the ICA (aka CCA, UCC) or the ICA member "CyberCaliphate," which have operated from September 2015 to the present.

A variety of factors cast doubt on the CyberCaliphate persona's claimed ISIS affiliation. For example, we did not observe official Islamic State media outlets commenting on any of CyberCaliphate's activity immediately following incidents. Other than general positive statements, we also did not observe ISIS sympathizers make specific comments about the TV5Monde incident or any other CyberCaliphate compromise in the immediate aftermath. This contrasts sharply with social media reactions to prominent pro-ISIS hacktivist activity, such as that conducted by the group Islamic State Hacking Division (ISHD), as well as kinetic attacks attributed to ISIS. ISIS supporters are well coordinated online, and mobilize rapidly following significant incidents to spread word. The lack of viral support for CyberCaliphate activities suggests that the operators behind the persona were not connected to pro-ISIS online communities. We believe that open source reports at the time claiming that Junaid Hussain (now deceased) was the leader of "CyberCaliphate" and that "CyberCaliphate" was directed or officially linked to the leadership of the Islamic State were unfounded, due to the lack of engagement between CyberCaliphate and the pro-ISIS online community. Hussein himself also denied such a connection.

TIMELINE OF ACTIVITY


2014
DEC 24

CyberCaliphate claims to deface the Albuquerque Journal website with a black and white image featuring a person wearing a kiffayah scarf wrapped around the head, an image of the Islamic State flag and the words "i love you isis [sic]." The image was accompanied by the text "CHRISTMAS WILL NEVER BE MERRY ANY LONGER"

DEC 29

CyberCaliphate claims to leak a database of Albuquerque Journal subscribers via Pastebin along with the message "NEW YEAR WILL MAKE YOU SUFFER INFIDELS" and statements denouncing the US-led bombing campaign against ISIS

2015
JAN 6

CyberCaliphate claims to compromise Albuquerque Journal and WBOC Maryland social media accounts, and to leak documents from the FBI; we assess that the attackers misrepresented the source of the documents. For instance, a significant portion of the documents appear to be official documents such as invoices, contracts, and reports from Stewart County, TN

JAN 12

CyberCaliphate compromises social media accounts of US Central Command (CENTCOM) and claims to have leaked documents from the Pentagon, including contact sheets for Army officers, policy documents such as slides and briefing memos, and slides that appear to have come from the MIT Lincoln Laboratory. While some of the documents came from open sources, we assess with low confidence that some of the documents contained moderately sensitive information, such as the Army officers' PII

JAN 23

APT28 first gains access to TV5Monde systems on this date, according to French authorities⁴⁵

FEB 10

The domain cyb3rc.com is registered

FEB 10

CyberCaliphate compromises social media accounts belonging to Newsweek and the Latin Times, defaces the website of the International Business Times, and claims to have leaked confidential documents from the "US National Cybersecurity Center." We assess with low confidence that CyberCaliphate successfully exfiltrated several documents from the Defense Cyber Investigations Training Academy (DCITA) and combined those with open source documents

APR 8

CyberCaliphate compromises social media accounts, defaces the website, and disrupts the broadcast of French TV station TV5Monde, warning the French military to "Stay out of Islamic State! Take a chance to save your families! [sic]." CyberCaliphate further claims to have leaked "confidential" documents from the French government, as well as identity documents of French soldiers. We assess with low confidence that CyberCaliphate successfully exfiltrated materials from several low- to moderate-profile French municipal government sources, and compiled them into a single dump

AUG 22

CyberCaliphate posts a response on their website to a Recorded Future article about the persona. This was the last observed public communication from CyberCaliphate

⁴⁵ <http://www.bbc.com/news/technology-37590375>

1.7.2: CyberBerkut



Period of Activity:
FEBRUARY 2014 - PRESENT

Appropriated Brands:
BERKUT (FORMER UKRAINIAN RIOT POLICE), ANONYMOUS

Websites:
CYBER-BERKUT.COM, CYBER-BERKUT.RU, OTHERS

Activity:
DDOS, DATA LEAKS, DATA DESTRUCTION, DEFACEMENTS, CREDENTIAL COMPROMISES

Known Tools:
VOLUNTARY DDOS BOTNET MALWARE, PHP SHELLS

Confidence in Russian State Sponsorship:
MODERATE

CyberBerkut (КиберБеркут) first emerged in early March 2014 – after the Ukrainian Maidan protests caused former Ukrainian President Yanukovich to flee the country but prior to Russia annexing Crimea. The group presents itself as sympathetic to Russian Government interests, and has conducted cyber threat activity in response to events related to the ongoing crisis between Russia and Ukraine over Crimea and the contested Donbass region. The CyberBerkut name is a reference to the Berkut, a Ukrainian special police unit that supported Yanukovich, which has been accused of killing unarmed protesters during the Euromaidan protests.

CyberBerkut's activity from March to August 2014 employed a variety of tactics, including DDoS attacks, defacements, and less frequently, telephony denial of service (TDoS) attacks, DNS hijacks, network intrusions, and data destruction. In contrast, CyberBerkut's activity from September 2014 to the present primarily consisted of claiming responsibility for various data leaks, some of which we believe to have been altered or entirely falsified. These data leaks and the group's accompanying messaging suggest that CyberBerkut's goal has been to influence public opinion and to undermine the Ukrainian Government. CyberBerkut most frequently targets Ukrainian Government officials and organizations and other individuals perceived to be linked to the Ukrainian Government, including NGOs, journalists, and commercial entities. The group has also targeted online assets of NATO and the governments of Germany, Poland, and the United States.

In contrast to the other personas discussed in this report, CyberBerkut exhibits some characteristics that suggest it might be an independent hacktivist group acting upon a pro-Russia motivation. For instance, unlike the other personas, for which there is little if any history, there is information available – albeit of dubious reliability – about individual CyberBerkut members, including with regards to alleged arrests and feuds between them. For example, an actor using the name “PravyjSektorUANationalistsUkraineAnon” claimed to have “doxed” four members of CyberBerkut in January 2015, posting names, aliases, social media accounts, and other information about the alleged members of CyberBerkut to Pastebin. One of the alleged members of CyberBerkut, “Mink,” also doxed fellow group members “MDV” and “artemova” in October and June 2014, respectively, apparently after a falling out. In February 2015, the @CyberBerkut Twitter account announced that MDV had been arrested.

Nonetheless, evidence of a connection between CyberBerkut and the Russian Government reduces the plausibility of CyberBerkut being wholly independent:

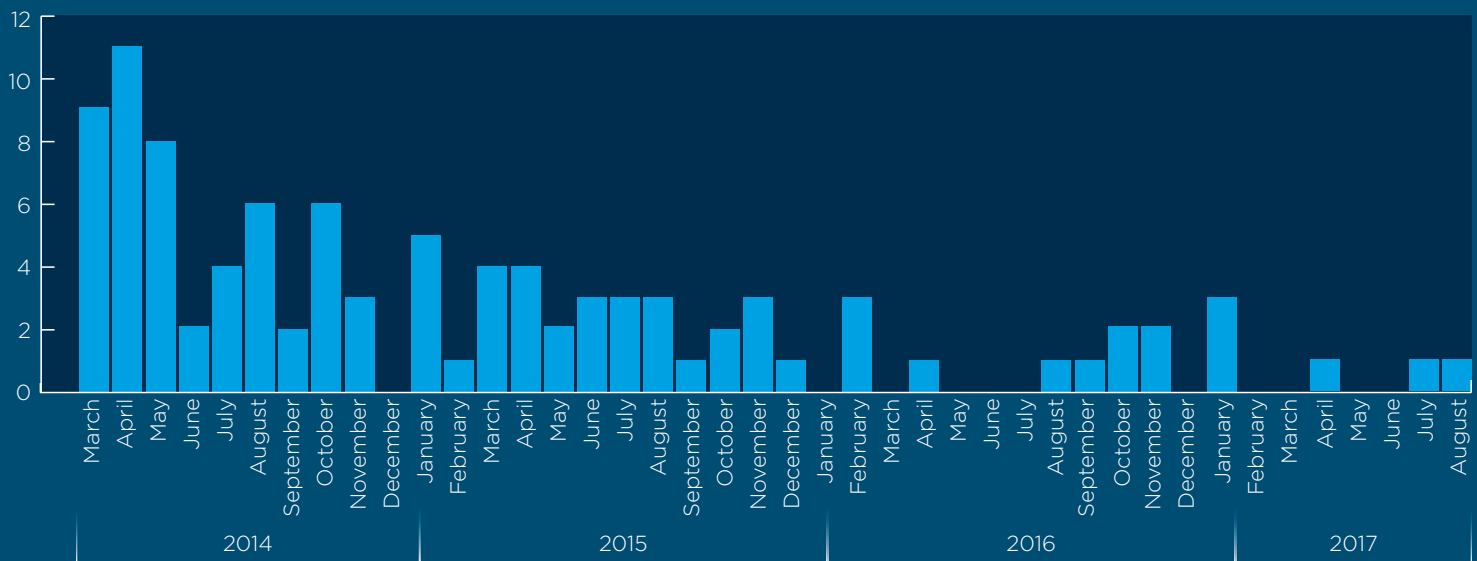
- During the May 2014 Ukrainian Presidential election, CyberBerkut claimed it had conducted a series of malicious activities against the Ukrainian Central Election Commission (CEC), including a system compromise, data destruction, a DDoS attack, and a leak of CEC network diagrams, employee logins, and other data. Ukrainian officials later revealed that the investigation into the compromise of the CEC's network identified the presence of APT28 malware.⁴⁶

⁴⁶ <http://www.nbcnews.com/mach/technology/election-cyberattacks-pro-russia-hackers-have-been-accused-past-n673246>

- In October 2016, CyberBerkut claimed to have leaked documents from the National Endowment for Democracy (NED) purportedly demonstrating that NED "sponsored a bloody civil war in Ukraine" working with reporter David Satter, who allegedly orchestrated anti-Russian propaganda through Radio Liberty and Russian opposition media outlets. Researchers at CitizenLab,⁴⁷ who examined the phishing email that was sent to David Satter, found that characteristics of the phishing email, the shortened link prompting the target to click, the pattern of redirects to the credential collection page, and the IP address used to host the credential collection page matched hallmarks of a phishing campaign targeting Bellingcat researchers that ThreatConnect⁴⁸ had analyzed and attributed to APT28.
- On August 23, 2017, CyberBerkut claimed to have leaked emails from the head of a Kiev-based NGO that allegedly demonstrate that the US tests biological weapons in Ukraine. Among the leaked emails, we observed what appeared to be four phishing messages, which we linked to tactics and phishing infrastructure controlled by APT28.
- On July 10, 2015, CyberBerkut claimed to have gained unauthorized access to US Senator John McCain's laptop during a visit to Ukraine, and posted a video allegedly demonstrating that the ISIS execution of James Foley was staged. The video was debunked as a fake.⁴⁹ Notably, this type of video production is not typical of hacktivist groups, and also indicates access to resources, such as studios, props, actors, and costumes, that is also not typical of hacktivist groups.

The exact nature of the relationship between CyberBerkut and the Russian Government is still unclear. It is plausible that CyberBerkut began as an independent hacktivist group but was later co-opted by Russian government-linked actors, or that the Russian Government maintains a more informal relationship with the group, providing leads, suggestions, maybe even support, but unofficially and through intermediaries. It is also plausible that CyberBerkut was Government-affiliated from inception, and that it differs in form from the other personas due to having been developed much earlier or having been designed for a different, more long-term purpose.

COUNT OF CYBERBERKUT THREAT ACTIVITY CLAIMS PER MONTH, MARCH 2014 - AUGUST 2017

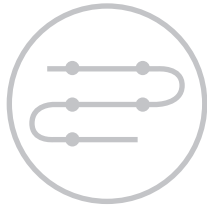


⁴⁷ <https://citizenlab.org/2017/05/tainted-leaks-disinformation-phish/>

⁴⁸ <https://www.threatconnect.com/blog/russia-hacks-bellingcat-mh17-investigation/>

⁴⁹ <https://www.metabunk.org/debunked-cyberberkut-video-supposedly-showing-staged-isis-beheading-of-foley.t6520/>

TIMELINE OF 2016-2017 ACTIVITY


2016
JAN 3

CyberBerkut claims to have accessed Android phones belonging to Ukrainian fighters in the "Azov" battalion, and posts a video and photos allegedly providing evidence that ISIS militants are fighting with Ukrainians against the Donetsk separatists. The video, photos, and claims of alleged ISIS involvement were later debunked by the BBC⁵⁰

FEB 10

CyberBerkut defaces the Bellingcat website.⁵¹ Bellingcat is an investigative journalism and research group that contributed to the MH-17 investigation

FEB 19

CyberBerkut claims to leak a document drafted by the head of the Foreign Intelligence Service of Ukraine containing plans to coerce Dutch officials ahead of the April 6, 2016 referendum in the Netherlands to approve or disapprove of the Association Agreement between the European Union and Ukraine

FEB 24

CyberBerkut leaks PII and personal photos of Ruslan Leviev, a blogger and Bellingcat researcher who has written articles critical of the Kremlin

APR 1

CyberBerkut leaks documents allegedly belonging to a Ukrainian parliamentary delegation that visited Belgium and the Netherlands. The veracity of documents is unconfirmed

APR 4

CyberBerkut claims to have maintained access to the network of the Ukrainian President's administration and leaks an alleged decree to "gift" a Ukrainian oblast to Turkey and Crimean Tatars for settlement. This document is likely fake

AUG 1

CyberBerkut claims to have leaked documents from the Turkish Ministry of Defense and Foreign Intelligence service allegedly demonstrating that the Turkish Government provides financial support to Tatar militants in Crimea. The authenticity of these documents is unconfirmed

SEP 1

CyberBerkut claims to have leaked documents from the Ukrainian Government allegedly exposing a Ukrainian effort to destroy evidence that the Security Service of Ukraine (SBU) had engaged in torture of detainees ahead of a visit by the United Nations Subcommittee on Prevention of Torture (SPT). The authenticity of the documents is unconfirmed

OCT 4

CyberBerkut claims to have leaked documents from the Ukrainian Government allegedly demonstrating that Ukrainian security agencies were obstructing Organization for Security and Cooperation in Europe (OSCE) monitoring efforts in Ukraine, that the Ukrainian State Border Guard Service was involved in smuggling petroleum products into Europe, and that the Ukrainian Government was also involved in "legalizing" ISIS militants and allowing them to travel into Europe. The authenticity of these documents is unconfirmed

OCT 22

CyberBerkut claims to have leaked documents from the National Endowment for Democracy (NED) purportedly demonstrating that NED "sponsored a bloody civil war in Ukraine" working with reporter David Satter, who allegedly orchestrated anti-Russian propaganda through Radio Liberty and Russian opposition media outlets. CitizenLab has since provided a detailed account of how the leaked documents were altered by CyberBerkut so that the group, and other Russian media outlets, could use them to support politically expedient narratives⁵²

NOV 4

CyberBerkut claims to have leaked documents allegedly belonging to Boris Lozhkin, the former head of the Ukrainian Presidential Administration, that allegedly demonstrate a conspiracy between the Kiev government and US State Department employees whom the persona claims to be sympathetic to the US Democratic Party, to expose evidence regarding Paul Manafort's work with former Ukrainian President Yanukovich in order to provide Hillary Clinton a political advantage. At least some of the documents appear to have been fabricated

NOV 27

CyberBerkut posts a transcripts of an alleged phone call between former US Vice President Joe Biden and Ukrainian President Petro Poroshenko in which Biden purportedly claimed an International Monetary Fund (IMF) payment to Ukraine was linked to the nationalization of PrivatBank. CyberBerkut claims that this demonstrates that the US Government is controlling Ukrainian oligarchs. The authenticity of the transcript is unconfirmed

⁵⁰ http://www.bbc.com/russian/features-38109630?ocid=socialflow_twitter

⁵¹ <https://twitter.com/bellingcat/status/697334674029412353>

⁵² <https://citizenlab.org/2017/05/tainted-leaks-disinformation-phish/#part2>

2017

JAN 13

CyberBerkut posts an image of an email allegedly exchanged between US officials revealing plans to falsify technical evidence in the US Government's January 2017 publicly released reports regarding Russian hacking and the 2016 presidential election.⁵³ The authenticity of this email is unconfirmed, and would not be difficult to fabricate

JAN 15

CyberBerkut claims to have leaked mail from a Polish Consul, emails from the German police, and documents from the Ukrainian Ministry of Internal Affairs (MIA), though the post was subsequently deleted from the group's website and social media outlets

JAN 16

CyberBerkut claims to have leaked additional documents from the Ukrainian MIA, some of which relate to Interior Minister Arsen Avakov. Also among the leaked documents is at least one email exchanged between Ukrainian MIA employees and a Latvian police officer. One screenshot appears to show that the perpetrators have access to a Zimbra collaboration software administrator page, lending some credence to the authenticity of at least some of the documents. Information about this alleged compromise was also subsequently removed from CyberBerkut's websites and social media outlets

APR 26

Media outlet LIFE posts a document allegedly stolen by CyberBerkut that discussed an incident in which a schoolboy traded alcohol for a grenade with a Ukrainian soldier.⁵⁴ No official CyberBerkut outlets reported this incident.

JUL 12

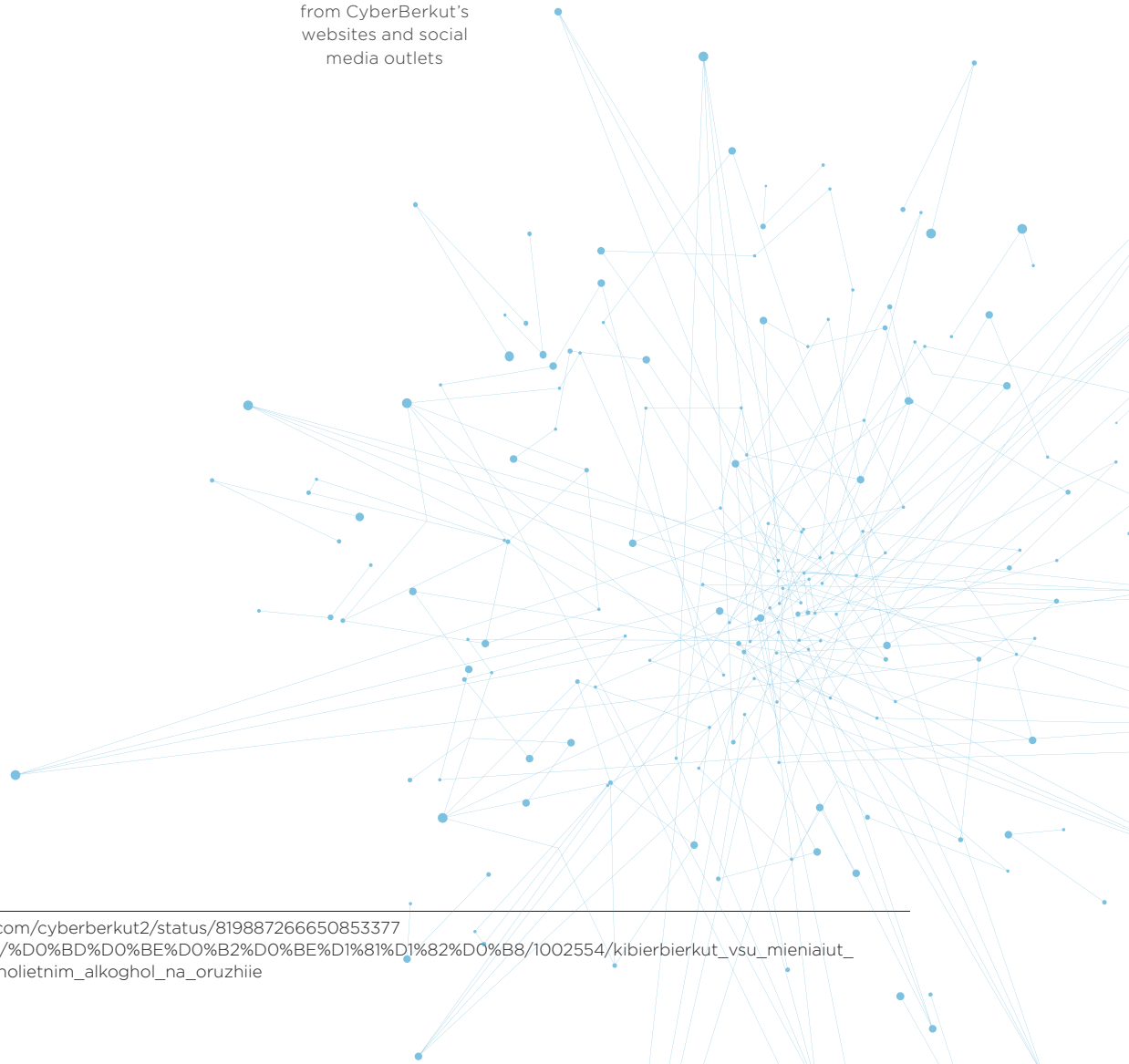
CyberBerkut claims to leak emails from the head of the board of a Ukrainian philanthropic organization that allegedly demonstrate links between Hillary Clinton's presidential campaign funds and a Ukrainian money laundering operation purportedly involving International Monetary Fund (IMF) loans intended for the Ukrainian Government

AUG 23

CyberBerkut claims to leak emails from the head of a Kiev-based NGO that allegedly demonstrate that the US tests biological weapons in Ukraine. Among the leaked emails, we observed what appeared to be four phishing messages, which we linked to tactics and phishing infrastructure controlled by APT28

⁵³ <https://twitter.com/cyberberkut2/status/819887266650853377>

⁵⁴ https://life.ru/t/%D0%BD%D0%BE%D0%B2%D0%BE%D1%81%D1%82%D0%B8/1002554/kibierbierkut_vsu_mieniaiut_niesoviershiennolietnim_alkoghol_na_oruzhiie



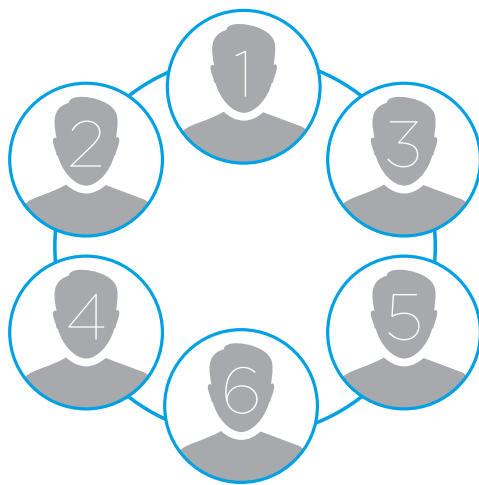
Part Two: Attribution

📍 MOSCOW



Assessment 3

Our assessment that the influence activity conducted by the six false personas in 2016 was Russian state-sponsored is based on its overlap with intrusion activity conducted by the Russian cyber espionage group APT28, other technical and circumstantial indications of Russian operators behind individual incidents, and uncanny similarities in the promotional behavior of the personas that tie them together.



Overt activity conducted by the Guccifer 2.0, DC Leaks, @anpoland, and Fancy Bears' Hack Team personas overlaps directly with covert intrusion and other malicious activities that FireEye and other security companies have attributed to the Russian cyber espionage group we track as APT28. We do not imply that the APT28 intrusion operators are the same operators behind the personas and their public-facing activity. Given the economics of resource allocation and the disparate skillsets employed, we suspect that these functions were likely segregated, with the actors responsible for compromising systems and obtaining sensitive data passing this on to a separate set of actors specializing in curation and dissemination. However, we do not have further insight into the specific entity or entities tasked with this dissemination function.

Connections to APT28 are weaker with regards to the @pravsector and Bozkurt Hackers personas; however, other indications point to Russian-speaking actors having been responsible for obtaining the data those personas subsequently leaked. One hypothesis we are currently exploring is that the intrusion operators that provided data to @pravsector and Bozkurt Hackers are an example of the often blurred boundary between official government actors and criminal actors coopted by the state. Uncanny similarities in leak dissemination behavior between the @anpoland, Fancy Bears' Hack Team, @pravsector, and Bozkurt Hackers personas lead us to assess that all four were controlled by the same actor(s) (see Part Three). Collectively, we suggest, this is indicative of a centralized information operations apparatus collating and disseminating data obtained via multiple intrusion operators.

When examined collectively, we believe that the sheer volume of individual circumstances and clues pointing to Russian state sponsorship constitute an insurmountable threshold that renders implausible alternative attribution scenarios.

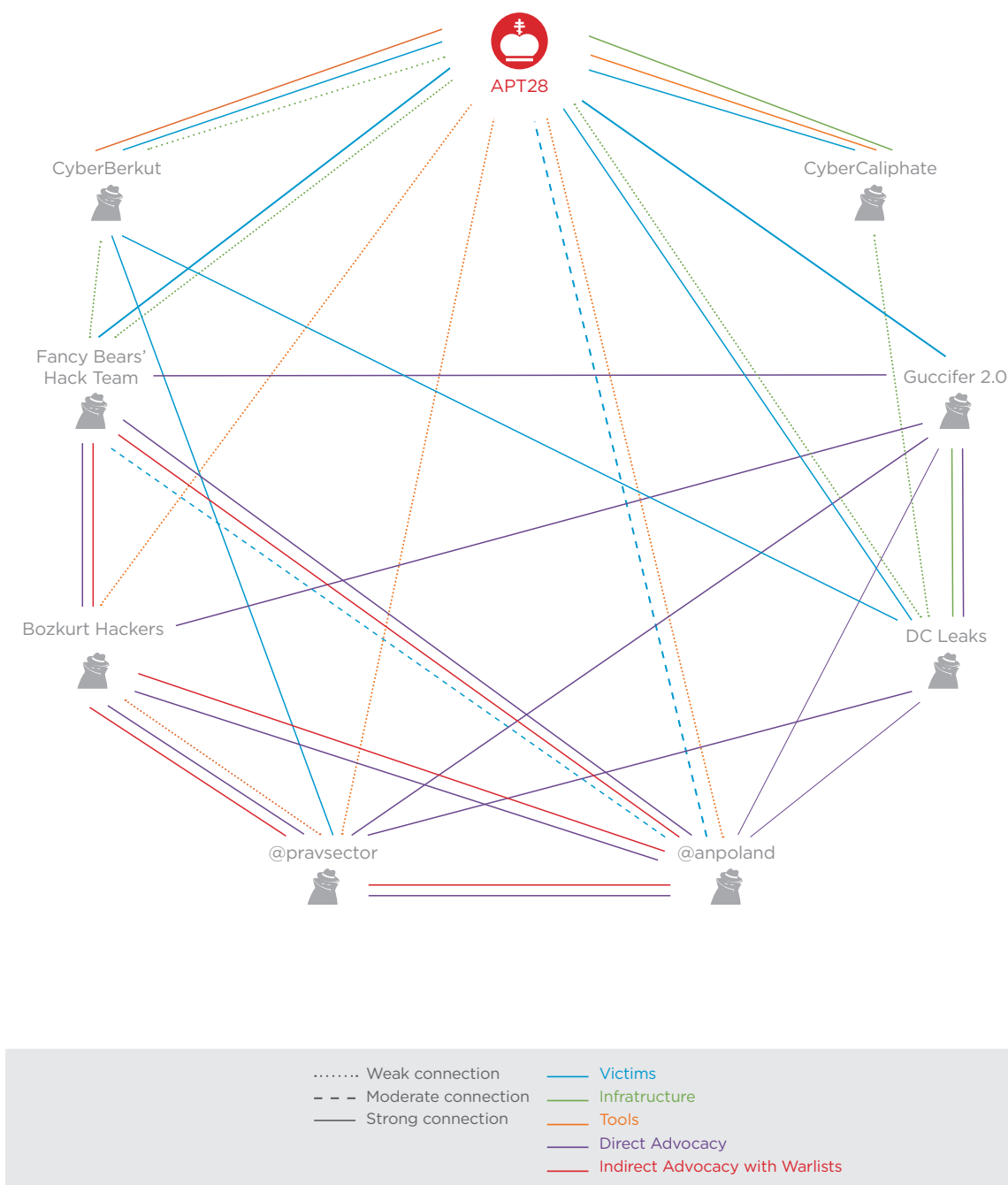


FIGURE 2.1: SUMMARY OF CONNECTIONS BETWEEN FALSE HACKTIVIST PERSONAS AND APT28, AND AMONG THE FALSE HACKTIVIST PERSONAS

Section 2.1: Overlaps with APT28



In January 2017, FireEye released *APT28: At the Center of the Storm*,⁵⁵ an update to our 2014 report⁵⁶ on the prolific cyber espionage group we assess to be Russian Government-sponsored. Those reports detail how and why we attribute APT28 to the Russian Government. Aspects of the influence activity discussed in this report can be tied to APT28 compromises, providing important indicators of Russian Government sponsorship behind the false hacktivist personas.

For example, the DC Leaks, Guccifer 2.0, and Fancy Bears' Hack Team personas were used to leak documents and other materials purportedly stolen from organizations that numerous researchers, including those at FireEye, have assessed were the victims of APT28 compromises, including the DNC, DCCC, WADA, and individuals including Clinton campaign chairman John Podesta and Former Secretary of State Gen. Colin Powell.

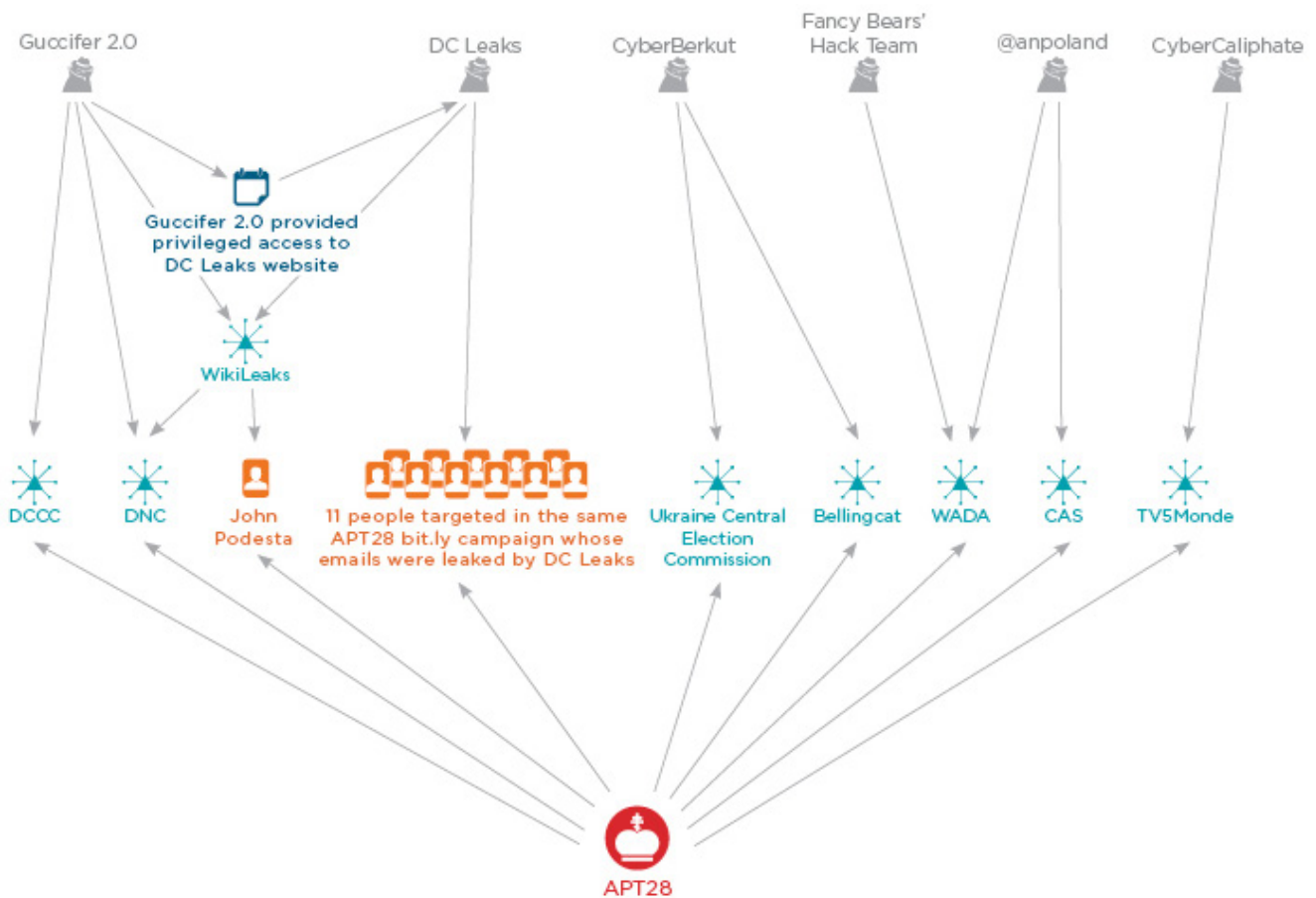


FIGURE 2.1.1: SHARED VICTIMOLOGY BETWEEN PERSONAS AND APT28

⁵⁵ <https://www2.fireeye.com/WEB-2017-RPT-APT28.html>

⁵⁶ <https://www2.fireeye.com/apt28.html>

We have also noted circumstantial evidence that is consistent with the hypothesis that the false hacktivist personas are linked to APT28 and/or the Russian Government, but independent of the more substantial evidence alluded to above (and detailed below), these indicators are inconclusive. For instance, we have documented similarities in infrastructure

procurement behavior, as well as overlaps in the use of particular open source tools by APT28 and some of the personas. While it is impossible to draw conclusions regarding attribution based on these circumstantial observations alone, when compiled with all other evidence, we believe the consistencies are noteworthy to highlight here for further investigation.

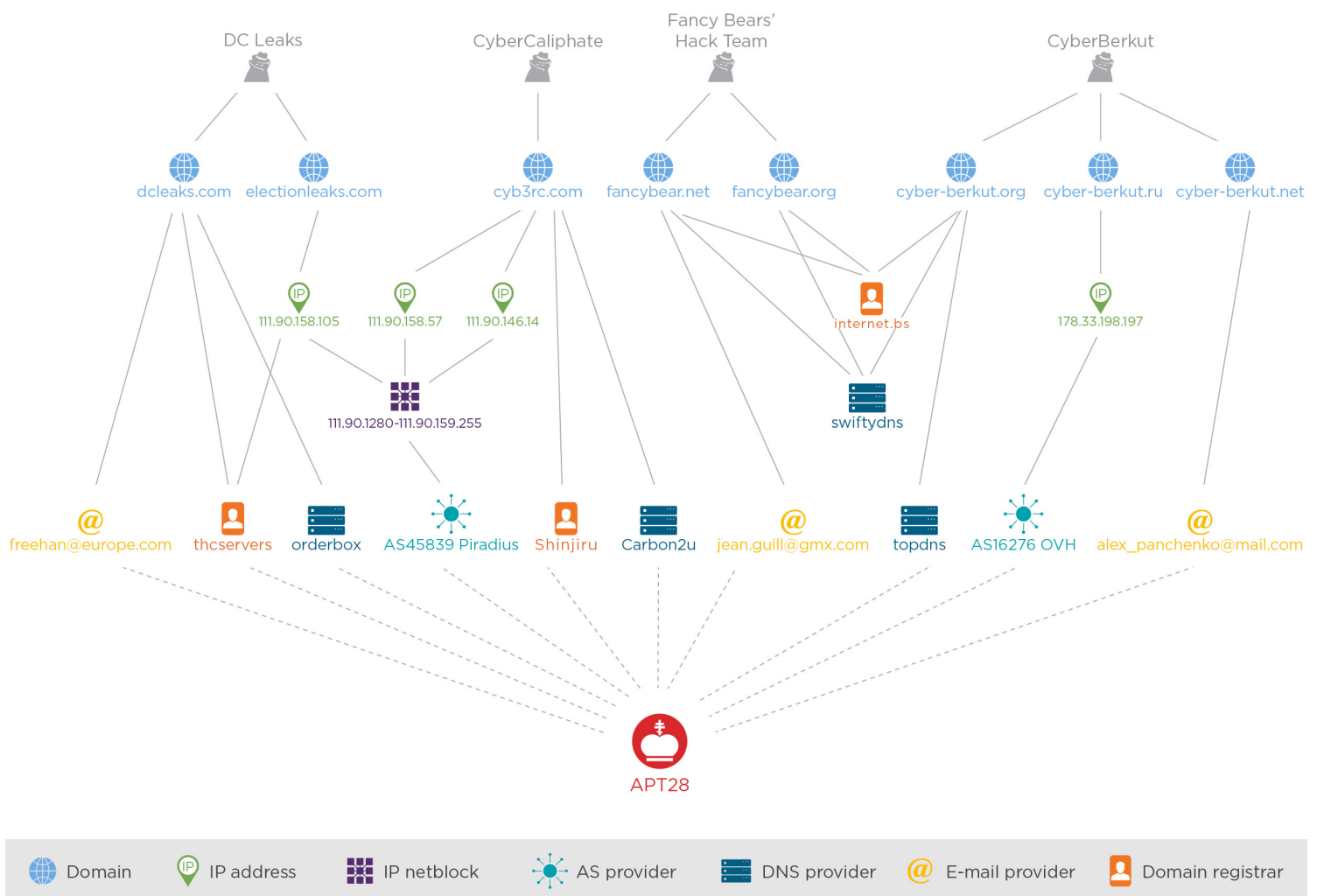


FIGURE 2.1.2: SIMILARITIES IN DOMAIN REGISTRATION BEHAVIOR BETWEEN PERSONAS AND APT28

Overlaps with APT28



Guccifer 2.0

- On June 14, 2016, the Democratic National Committee (DNC) announced it had suffered network compromises earlier in the year and that a subsequent investigation had identified APT28 and APT29, two Russian cyber espionage actors, as the perpetrators of two separate intrusions into DNC systems. FireEye analyzed malware samples purportedly found on DNC networks and determined that these were consistent with our previous observations of APT28's X-Tunnel and CHOPSTICK tools and APT29's SEADADDY tool.⁵⁷ The following day, the Guccifer 2.0 persona claimed responsibility for the DNC breach, and began leaking documents taken from the organization's network as evidence.⁵⁸ The persona continued to post batches of DNC documents though October.⁵⁹
- In July 2016, the Democratic Congressional Campaign Committee (DCCC) announced that it was investigating an ongoing "cybersecurity incident" that the FBI considered to be part of the same incident as the APT28 compromise of the DNC.⁶⁰ Investigators indicated that the perpetrators may have gained access to DCCC systems as early as March.⁶¹ FireEye reported that APT28 had compromised fundraising components of the DCCC website in June, redirecting visitors to a site controlled by the group. In August 2016, the Guccifer 2.0 persona contacted reporters covering US House of Representative races to promote newly leaked documents pertaining to Democratic candidates. Between August and October, the persona posted several additional installments of what appear to be internal DCCC documents on the Guccifer 2.0 WordPress site.^{62, 63}



DC Leaks

- In June 2016, Dell SecureWorks published a report describing a wide-ranging phishing campaign they attributed to APT28, in which targets were sent emails masquerading as legitimate communications from Google prompting recipients to reset their Gmail passwords by clicking on a shortened bit.ly link. In addition to traditional APT28 targets, such as US and European Government and military personnel, contractors, and journalists, the targets of this campaign also included Hillary Clinton, her campaign staff, and DNC staff.⁶⁴ The credential collection page used in the phishing email sent to John Podesta was hosted on a domain we have previously associated with APT28.
- Most of the individuals from whom DC Leaks leaked e-mails were reportedly victims of this same APT28 bit.ly campaign: Philip Breedlove, Sarah Hamilton, Brian Keller, Zachary Leighton, Capricia Marshall, Ian Mellul, Bianca Nicholson, Carl Pistole, Colin Powell, Sarah Stoll, William Rinehart, and John Podesta.⁶⁵
- The domains dcleaks.com were hosted on the Piradius autonomous system (AS), and dcleaks.com and electionleaks.com used nameservers at thcservers.com. The dcleaks.com domain also used nameservers at orderbox.com, and was registered using an europe.com email address. We have previously observed APT28 using all of these services. dcleaks.com also uses an IP in the same Piradius-owned bloc as the IP that was used by the CyberCaliphate website.

⁵⁷ https://www.washingtonpost.com/world/national-security/cyber-researchers-confirm-russian-government-hack-of-democratic-national-committee/2016/06/20/e7375bc0-3719-11e6-9ccd-d6005beac8b3_story.html

⁵⁸ <http://motherboard.vice.com/read/all-signs-point-to-russia-being-behind-the-dnc-hack>

⁵⁹ <http://www.politico.com/story/2016/10/dnc-trump-steaks-hackers-229954>

⁶⁰ https://www.washingtonpost.com/world/national-security/fbi-probes-suspected-breach-of-dccc-computers-by-russian-hackers/2016/07/28/71210464-5536-11e6-b7de-dfe509430c39_story.html

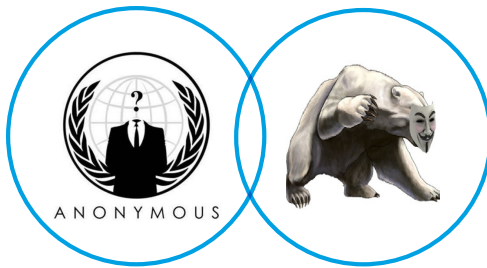
⁶¹ <http://www.nytimes.com/2016/12/13/us/politics/house-democrats-hacking-dccc.html>

⁶² <http://www.nytimes.com/2016/12/13/us/politics/house-democrats-hacking-dccc.html>

⁶³ <http://arstechnica.com/security/2016/10/guccifer-2-0-posts-dccc-docs-says-theyre-from-clinton-foundation/>

⁶⁴ <https://www.secureworks.com/research/threat-group-4127-targets-hillary-clinton-presidential-campaign>

⁶⁵ <https://www.intelligence.senate.gov/sites/default/files/documents/os-trid-033017.pdf>



@anpoland and Fancy Bears' Hack Team

- We believe that APT28 is associated with malicious infrastructure that spoofed the World Anti-Doping Agency (WADA) and the Court of Arbitration for Sport (CAS). The domains wada-awa.org and wada-arna.org (registered on Aug. 3 and Aug. 8, 2016, respectively) spoofed the legitimate website of WADA, wada-ama.org. The domain tas-cass.org (registered on Aug. 8) spoofed tas-cas.org, the CAS website. All three spoofed domains were registered through IT Itch, a registrar that accepts Bitcoin and that FireEye has previously seen leveraged by APT28. Wada-awa.org and tas-cass.org both resolved to 81.95.5.166 (AS201011). FireEye has identified the same subnet as having been previously linked to multiple APT28 domains.
- On Aug. 10, 2016, @anpoland claimed to have leaked data from CAS and to have defaced the websites of CAS and WADA. @anpoland also threatened to release data from WADA on Aug. 11 and Sept. 5, but failed to follow through on this threat.
- On September 12, 2016, Fancy Bears' Hack Team claimed to have compromised WADA and released athlete medical records as "proof of American athletes taking doping."⁶⁶ On September 13, WADA confirmed that APT28 had compromised its networks and accessed athlete medical data, which was then publicly released.⁶⁷ From September 15–30, 2016, Fancy Bears' Hack Team released five additional batches of medical files of top athletes from multiple nations.
- On April 3, 2017, the International Association of Athletics Federations (IAAF) disclosed that it had suffered a compromise by APT28, that evidence of APT28 activity was noted as early as Feb. 21, 2017, and that the attackers had accessed metadata relating to athlete Therapeutic Use Exemptions (TUEs).⁶⁸ On July 5, 2017, Fancy Bears' Hack Team claimed to have leaked data, specifically emails and attachments, from IAAF regarding alleged athlete doping violations and other purported unethical or unfair behavior by anti-doping bodies. Though IAAF did not discuss a compromise of emails in their public release, it is plausible that APT28 accessed additional IAAF systems, and the timeframe for the leaked emails matches the dates of APT28 access revealed by IAAF.



@pravsector

- There is broad overlap between @pravsector and APT28 targeting patterns; both have targeted the Ukrainian Government, the US Government, US defense industrial base companies, and the Polish Government.

⁶⁶ <https://twitter.com/fancybears/status/775472072650788864>

⁶⁷ <https://www.wada-ama.org/en/media/news/2016-09/wada-confirms-attack-by-russian-cyber-espionage-group>

⁶⁸ <https://www.iaaf.org/news/press-release/iaaf-cyber-attack>



CyberCaliphate

- In February 2015, FireEye discovered a variant of the APT28 CORESHELL downloader, an updated version of the group's prolific SOURFACE (aka Sofacy) tool, that was configured to call out to two command and control (C&C) domains. Through monitoring one of the C&C domains, we identified CORESHELL traffic beaconing from French television outlet TV5Monde's network, confirming that it was the victim of an APT28 compromise. In April 2015, CyberCaliphate claimed responsibility for the destructive attack against TV5Monde.
- In June 2015, French newspaper L'Express published an article stating that French investigators were focusing on APT28 as the probable culprits behind the April "CyberCaliphate" attack.⁶⁹ The General Director of TV5Monde, Yves Bigot, confirmed they were focused on the Russian threat group and cooperating with French authorities.⁷⁰
- The CyberCaliphate website, cyb3rc.com, used the Shinjuru registrar and nameservers at carbon2u.com, and was hosted on the Piradius autonomous system (AS). These web services are favorites of APT28.
- Through sensitive sources, we definitively tied activity surrounding cyb3rc.com to activity surrounding jihadkavkaz.com, chmail.in, and other domains we know to belong to APT28.



CyberBerkut

CyberBerkut and APT28 have targeted several of the same individuals and organizations. In two cases, those of the Ukrainian Central Election Commission and Bellingcat, we have evidence that CyberBerkut and APT28 targeted these organizations in the same time frame. In two phishing incidents—that of a phishing email sent to journalist David Satter,⁷¹ and a more recent case of a phishing message sent to a Ukrainian NGO head—there is evidence to tie APT28 intrusion activity to CyberBerkut data leaks.

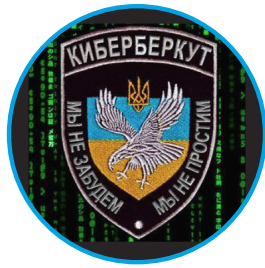
- During the May 2014 Ukrainian Presidential election, CyberBerkut conducted a variety of activities against the Ukraine Central Election Commission (CEC), including gaining unauthorized access, destroying data, leaking data, and conducting a DDoS attack against the CEC website. In June 2016, Ukrainian officials revealed that an investigation into the compromises identified APT28 malware (Sofacy) in the CEC's internal network,⁷² however public statements from officials and Ukraine CERT did not specifically state that the Sofacy samples found at the CEC were directly tied to the other election-day compromises, including those claimed by CyberBerkut. It is possible that the investigators chose not to disclose whether they suspected the presence of more than one set of attackers or that the investigation was inconclusive. CyberBerkut claimed to have used a zero-day to gain access to the CEC's systems, but in its post incident investigation, Ukraine CERT found that there were unpatched vulnerabilities in the server, and suggested that the attackers likely gained access due to misconfigured security settings.

⁶⁹ http://www.lexpress.fr/actualite/medias/piratage-de-tv5-monde-la-piste-russe_1687673.html

⁷⁰ <http://www.bbc.com/news/technology-37590375>

⁷¹ <https://citizenlab.org/2017/05/tainted-leaks-disinformation-phish/>

⁷² <http://www.nbcnews.com/mach/technology/election-cyberattacks-pro-russia-hackers-have-been-accused-past-n673246>



CyberBerkut (continued)

- Bellingcat is a network of investigative journalists who compile research based on open source data. On Feb. 10, 2016, CyberBerkut defaced Bellingcat's website using the credentials of Bellingcat contributor Ruslan Leviev, who has written articles critical of the Kremlin.⁷³ On Feb. 27, 2016, CyberBerkut also posted personal photos, emails, and PII of Leviev. ThreatConnect found that at least three Bellingcat researchers, Elliot Higgins, Aric Toler, and Veli-Peka Kivimaki, all of whom contributed to Bellingcat's investigation into the downing of Malaysia Airlines flight 17 over eastern Ukraine, were targeted in the same APT28 Gmail credential phishing campaign using bit.ly URLs identified by Dell Secure Works (discussed in the DC Leaks section above) from February 2015 to September 2016.⁷⁴ According to Bellingcat, however, none of the recipients of phishing emails provided credentials to the credential collection pages. The window for the APT28 phishing campaign overlaps with the February 2016 CyberBerkut compromises; however, we observed no evidence that Leviev's email was targeted in the bit.ly campaign. It is probable that Bellingcat would have sought to identify any additional phishing attempts and disclose them to ThreatConnect, though whether they were able to thoroughly check all contributors' personal email accounts or devices for other signs of targeting is unclear.
- In October 2016, CyberBerkut claimed to have leaked documents from the National Endowment for Democracy (NED) purportedly demonstrating that NED "sponsored a bloody civil war in Ukraine" working with reporter David Satter, who CyberBerkut alleged orchestrated anti-Russian propaganda through Radio Liberty and Russian opposition media outlets. Researchers at Citizen Lab,⁷⁵ who examined the phishing email that was sent to David Satter, found that characteristics of the phishing email, the shortened link leading to the credential collection page, and the IP address used to host the credential collection page, matched hallmarks of a phishing campaign targeting Bellingcat researchers that ThreatConnect⁷⁶ had analyzed and attributed to APT28.
- On August 23, 2017, CyberBerkut claimed to have leaked emails from the head of a Kiev-based NGO that allegedly demonstrate that the US tests biological weapons in Ukraine. Among the leaked emails, we observed what appeared to be four phishing messages, which we linked to tactics and phishing infrastructure controlled by APT28.
- The cyber-berkut.org domain used nameservers at topdns.com, the cyber-berkut.ru domain was hosted on the OVH autonomous system (AS), and several CyberBerkut domains were registered using a mail.com email address. APT28 has also used these services extensively.

⁷³ <https://twitter.com/bellingcat/status/697334674029412353>

⁷⁴ <https://www.threatconnect.com/blog/russia-hacks-bellingcat-mh17-investigation/>

⁷⁵ <https://citizenlab.org/2017/05/tainted-leaks-disinformation-phish/#part2>

⁷⁶ <https://www.threatconnect.com/blog/russia-hacks-bellingcat-mh17-investigation/>

Section 2.2: Other Indications of Russian Operator Involvement

In addition to evidence linking several of the false hacktivist personas to APT28, we have also observed other disparate indications of Russian-speaking operator involvement behind some of the personas. The most widely known of these relate to Guccifer 2.0's early leak activity, however the most extensive set of additional indications we observed relate to Bozkurt Hackers.

Additional Indications of Russian Operator Involvement



Guccifer 2.0

- According to Microsoft Word metadata, some of Guccifer 2.0's earliest claimed leaked DNC documents were modified by an individual using the pseudonym "Феликс Эдмундович", (Felix Edmundovich). Felix Edmundovich Dzerzhinsky was a Soviet statesman, known for establishing the Soviet secret police force.
- The PDF version of the Donald Trump opposition research report that Guccifer 2.0 provided to The Smoking Gun contains Russian error messages associated with several embedded links, reading "Ошибка! Недопустимый объект гиперссылки." However, the Microsoft Word version of the report published on Guccifer 2.0's WordPress blog contained those error messages in English, reading "Error! Hyperlink reference not valid." Given that the Word document contained the messages in English and that the author appears to be connected to the DNC, we surmise that the Word document was the original and that a Russian-speaking actor later saved that Word document as a PDF.



Bozkurt Hackers

- On August 16, 2014, an actor using the name "arhar" posted a message on a Russian-language hacking forum requesting assistance with decrypting a set of hashed passwords. We found these hashes among data Bozkurt Hackers claimed to have leaked from the Commercial Bank of Ceylon (ComBank) in May 2016, and a Havij output file also included in that leak indicates that these hashes were extracted from ComBank on August 16, 2014. The timing of arhar's post strongly suggests that this actor was involved in the ComBank compromise, or at least associated with the operators who exfiltrated the hashes.
- Among the files Bozkurt Hackers allegedly leaked from Qatar National Bank (QNB) were screenshots showing a user logged into a QNB fileshare system using a Russian-language version of the Firefox browser. The screenshots revealed that the perpetrators of the breach may have been operating from the IP addresses 188.64.173.3 (Russia) and 173.255.185.194 (US), though we were unable to determine the screenshots' authenticity.
- Opening leaked Excel spreadsheets from the Bozkurt Hackers claimed QNB, InvestBank, and Sanima Bank breaches revealed that in some cases the spreadsheets were labeled with the Russian word for sheet (Лист), indicating that the workbooks had previously been opened or saved on a computer using Russian as the default language.

**Bozkurt Hackers (continued)**

- Bozkurt Hackers posted four of its data dumps to the file sharing sites global-files.net or mf-arch.ru, which are hosted at the same IP address, 46.188.0.26 (Russia). Global-files.net and mf-arch.ru are used most frequently in Russia, and both are relatively obscure compared to other file sharing services, even within Russia. In each case, we observed at least some indication that Bozkurt Hackers attempted to obfuscate the connection to global-files.net, for instance, by building multiple redirects into links to the data downloads, or by using multiple URL shorteners to package the links. Notably, we observed that when the @Cryptomeorg Twitter account reported receiving a "service unavailable" error when attempting to open a Sanima Bank download link, Bozkurt Hackers instructed them to try again, but did not provide a new link. We suspect that the @Cryptomeorg operators were subsequently able to access the data, which would indicate that Bozkurt Hackers was at least in communication with the file sharing website administrator, if not in possession of direct back-end access themselves to make the original link available. The global-files.net domain is registered to a Moscow-based individual, Aleksandr Evgenevich Sukhodko (Александр Суходько, aka dalamar81). Notably, the @pravsector persona also used global-files.net to host the data purportedly stolen from Polish telecom Netia for public download.

**@pravsector**

- On Aug. 1, 2016, @pravsector posted a screenshot to demonstrate its access to an alleged "hacked mil[itary] pc." The screenshot included a window titled "connected to remote desktop" written in Russian rather than Ukrainian, suggesting that the actor operating this computer had set the default language to Russian.

Section 2.3: Additional Overlaps between Personas

We believe that substantial behavioral similarities and other overlaps exhibited between various subsets of the personas provide additional indications of shared operators or otherwise close affiliation.

- In section 3.3, we extensively detail striking similarities in dissemination behavior between the @anpoland, Fancy Bears' Hack Team, @pravsector, and Bozkurt Hackers personas, which engaged in a systematized dissemination technique we have termed Indirect Advocacy via Warlists to promote leaks and associated political narratives. This activity leveraged large networks of semi-automated Twitter accounts, presenting as unaffiliated with the personas, to push leaks and associated narratives to influential individuals in a highly-systematized manner via targeted messaging. The uncanny similarities between these four personas' indirect advocacy activity leads us to suspect that they were controlled by the same operator(s).
- As detailed in sections 1.3 and 1.4, @anpoland twice threatened to leak data from WADA, but failed to follow through on the threats. The Fancy Bears' Hack Team then surfaced and took credit for the WADA leaks that subsequently occurred, again suggesting close affiliation between the two personas.
- As also detailed in section 1.2, in June 2016 the Guccifer 2.0 persona approached The Smoking Gun journalist William Bastone with private credentials for content hosted on the DC Leaks website prior to its public disclosure, and claimed that DC Leaks was a "sub-project" by WikiLeaks, indicating a close relationship existed between the two personas.

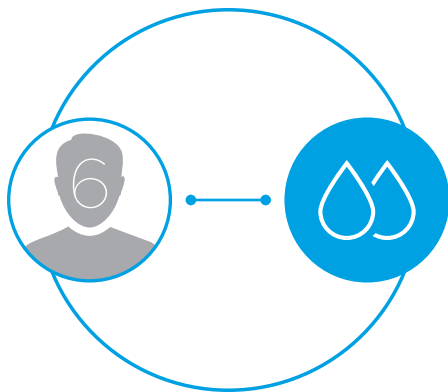


Part Three: Dissemination



Assessment 4

We assess with high confidence that the personas engaged in highly organized, systematized, and in some cases semi-automated social media dissemination campaigns to promote leaks and associated political narratives to media outlets and other influencers, in order to generate mainstream coverage and public attention.



This dissemination activity included what we have termed **Direct Advocacy**, whereby the personas directly targeted influential individuals such as journalists with promotional messaging, and **Indirect Advocacy via “Warlists,”** whereby large networks of semi-automated Twitter accounts, presenting as unaffiliated with the personas, similarly

pushed leaks and associated narratives to influential individuals in a highly systematized manner via targeted messaging. We suggest that this advocacy demonstrated, to at least some degree, a nuanced understanding of the personas’ target audiences. All six of the personas in 2016 engaged in some form of direct advocacy. Four of the personas – @anpoland, Fancy Bears’ Hack Team, @pravsector, and Bozkurt Hackers – engaged in strikingly similar instances of indirect advocacy via the use of Twitter Warlists. As we indicated in section 2.3, the uncanny similarities between these four personas’ indirect advocacy activity leads us to suspect that they were controlled by the same operator(s).

We have defined the “Warlist” moniker to mean cultivated networks of human-assisted bots (or “cyborg” accounts) designed to produce large-scale bursts of customized, politically-motivated messaging following inputs from a human operator. These Warlists exhibited several characteristics that we believe qualify them as a unique subset of bot activity, including the universal adoption of identical false identities – particularly those of media entities – by accounts within individual Warlists, and the organized manner of their promotional activity, with accounts posting thousands of times in alphabetical order following consistent schedules.

Assessment 5

We assess with high confidence that the operators behind the Guccifer 2.0 and DC Leaks personas also leveraged WikiLeaks in their effort to undermine Hillary Clinton's presidential campaign and the Democratic Party more broadly.

From the summer of 2016 through to US election day on November 8, the anti-secrecy organization WikiLeaks released thousands of documents purportedly stolen from the Democratic National Committee and the personal email account of Clinton campaign chairman John Podesta. These releases fed the proliferation of numerous narratives regarding a corrupt Hillary Clinton and disinformation intended to undermine her candidacy. We are unable to make a clear determination as to whether WikiLeaks knowingly and willingly colluded with Russia in these leaks, or was an unwitting partner that was passed the allegedly stolen data by a purported unaffiliated intermediary. Regardless of the nature of the relationship, WikiLeaks' statements and rhetoric indicate that the organization willingly and enthusiastically leaked data with the intention of undermining Clinton's presidential campaign. We assess that Russia opted to also leverage WikiLeaks as a publication vehicle due to the organization's high profile and perceived credibility.



Section 3.1: Platforms

Twitter Accounts

Dedicated Websites

WikiLeaks

3.1.1: Twitter Accounts

All six of the suspected false hacktivist personas used Twitter to publicize their activity, generating thousands of followers between them. As of May 2017, Guccifer 2.0's Twitter account had generated the highest number of followers, at over 46,000; DC Leaks and Fancy Bears' Hack Team (@FancyBears) also generated high follower counts, at over 13,000 and 8,500, respectively.

@anpoland's creation date is an anomaly for this set of accounts, and raises questions regarding the original operators and purpose of the account. Nonetheless, as noted in section 1.3, outside of one tweet in 2010 and two retweets in 2012, all activity from the @anpoland account occurred on and after July 29, 2016, placing it primarily within the same operating window as the other personas. The account's original tweet in 2010 possesses features that suggest the account may have originally been a news-promotion bot, however we are currently unable to make any further determination as to its origins.

PERSONA	ACCOUNT NAME(S)	CREATION DATE	ACCOUNT STATUS AS OF JUNE 2017
Guccifer 2.0	@GUCCIFER_2	6/20/2016	Accessible
DC Leaks	@dcleaks_	6/8/2016	Accessible
@anpoland (Anonymous Poland)	@anpoland	4/23/2010	Accessible
Fancy Bears' Hack Team	@FancyBears @FancyBearsHT	9/6/2016 9/12/2016	Accessible Accessible
@pravsector (Pravyy Sektor)	@pravsector @pravvysektor	7/1/2016* 6/1/2016*	Unavailable Unavailable
Bozkurt Hackers	@turkey_bozkurt @_bozkurtlar1923 @Bozkurthackers_ @BOZKURT_007_ @_bozkurt_1923 @ulkuocaklar1923 @bozkurthackers @bozkurt_1923_ @bozkurt_turk_ @_bozkurt1923 @BOZKURT_007_	4/17/2016 4/17/2016 4/20/2016 4/21/2016 Unknown Unknown Unknown Unknown Unknown Unknown Unknown	Accessible Accessible Accessible Accessible Unavailable Unavailable Unavailable Unavailable Unavailable Unavailable Unavailable

FIGURE 3.1.1: TWITTER ACCOUNTS USED BY SUSPECTED FALSE HACKTIVIST PERSONAS. DATES MARKED WITH "*" ARE LIKELY ACCURATE BUT CANNOT NOW BE CONFIRMED DUE TO ACCOUNT DELETION.

3.1.2: Dedicated Websites

As part of their brand appropriation efforts (see Part One), three of the personas, Guccifer 2.0, DC Leaks, and Fancy Bears’ Hack Team, established dedicated websites or blogs to promote their activity and publish allegedly leaked documents. In the case of DC Leaks, the dcleaks.com domain was registered in April 2016, two months prior to its first leak publications in June, demonstrating that the public-facing influence activity conducted by the persona was, to at least some degree, planned well in advance. As the Guccifer 2.0 website is a subdomain of WordPress, we do not know the exact date that the account was registered; the first activity on the site was on June 15, the date of the first of Guccifer 2.0’s leaks and the day immediately following CrowdStrike’s public attribution of the DNC breach. We suspect that the site was quickly put together that day as part of the broad effort to discredit CrowdStrike’s attribution (see section 1.1). The Fancy Bears’ Hack Team domains were registered 12 days before the persona began leaking data from WADA, and notably, prior to @anpoland’s second (Sept. 5) threat that it would leak data from the organization.

The use of dedicated websites facilitated the promotion of these three personas’ threat activity in key ways. First, the websites established an online presence that was arguably less susceptible to being shut down or otherwise censored compared to social media accounts. Second, and similarly, the websites allowed the personas to host allegedly leaked data directly, making it more difficult to take down or otherwise censor content than if hosted on third party platforms such as Pastebin or Mega. In both cases, these benefits were perhaps less true for the Guccifer 2.0 site, which was hosted on the WordPress platform rather than an independent server. Third, we suggest the websites and their branding helped reinforce perceptions of legitimacy and credibility as authentic hacktivist actors that the personas attempted to nurture.

The guccifer2.wordpress.com, dcleaks.com, and fancybear.net domains enjoyed sharp and significant spikes in web traffic during the height of their respective leaks, as measured by the site traffic ranking website Alexa. All three sites appeared within the top 100,000 websites in the world by traffic volume at various points between September and November 2016. Traffic volume for guccifer2.wordpress.com and dcleaks.com dropped sharply after November 2016, while traffic for fancybear.net continued to rise before dropping sharply in December 2016. Traffic volume to fancybears.net experienced a slight resurgence in August 2017.

WEBSITE	REGISTRATION DATE	PERSONA
guccifer2.wordpress.com	Unknown (suspected 6/15/2016)	Guccifer 2.0
electionleaks.com	4/12/2016	DCLeaks
dcleaks.com	4/19/2016	DCLeaks
dcleaks.net*	9/29/2016	DCLeaks (suspect affiliation)
fancybear.net	9/1/2016	Fancy Bears Hack Team
fancybear.org	9/1/2016	Fancy Bears Hack Team

FIGURE 3.1.2: WEBSITE DOMAINS FOR THE DCLEAKS, GUCCIFER 2.0, AND FANCY BEARS’ HACK TEAM PERSONAS. (*AS DETAILED IN THE DC LEAKS TIMELINE IN SECTION 1.2, DOMAIN REGISTRATION PATTERNS MAY SUGGEST THIS DOMAIN WAS NOT REGISTERED BY THE OPERATORS BEHIND THE DC LEAKS PERSONA BUT INSTEAD BY A THIRD PARTY SEEKING TO TAKE ADVANTAGE OF THE DC LEAKS BRAND).

3.1.3: WikiLeaks

We assess with high confidence that the operators behind the Guccifer 2.0 and DC Leaks personas also leveraged WikiLeaks in their effort to influence the 2016 US election cycle and undermine Hillary Clinton's presidential campaign and the Democratic Party, in concurrence with a conclusion reached by the US Intelligence Community in a January 2017 assessment of this activity.⁷⁷ From the summer of 2016 through to US election day on Nov. 8, WikiLeaks released thousands of documents purportedly stolen from the DNC and the personal email account of Clinton campaign chairman John Podesta. These releases fed the proliferation of numerous narratives regarding a corrupt Hillary Clinton and disinformation intended to undermine her candidacy.

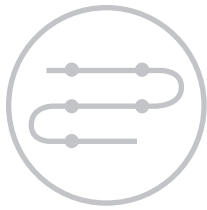
Although we did not observe any persona claim credit for the Podesta email compromise, the correspondence of other individuals compromised in the same phishing campaign, which Dell SecureWorks attributed to APT28, such as Colin Powell and Clinton campaign staffer William Rinehart, were published on the DC Leaks website, suggesting a link between these sets of activity.⁷⁸ WikiLeaks also published allegedly stolen DNC documents after the Guccifer 2.0 persona claimed to have passed them on. WikiLeaks' publication of purportedly stolen emails and other documents continued unabated daily from the second week of October right up until the day before the US elections.

We are unable to make a clear determination as to whether WikiLeaks knowingly and willingly colluded with Russia in these leaks, or was an unwitting partner that was passed the stolen data by a purported unaffiliated intermediary, unaware of the true source. Regardless of the nature of the relationship, WikiLeaks' statements and rhetoric indicate that the organization willingly and enthusiastically leaked data with the intention of undermining Clinton's presidential campaign. We assess that Russia opted to leverage WikiLeaks as a publication vehicle due to the organization's high profile, large audience reach, and perceived credibility, demonstrating a strong awareness of the popularity and newsworthiness of the brand. Wikileaks.org ranks in the top 5,000 websites by traffic volume in the world and in the top 1,000 in the US. Its supporters regularly credit the site with having never released a single falsified document, although this claim is disputed. WikiLeaks' publication of John Podesta's email correspondence generated immediate international media attention and appeared to influence much of the conversation regarding Hillary Clinton's campaign in the final month leading up to the presidential election.



⁷⁷ https://www.dni.gov/files/documents/ICA_2017_01.pdf

⁷⁸ <https://www.secureworks.com/research/threat-group-4127-targets-hillary-clinton-presidential-campaign>



TIMELINE OF ACTIVITY

2016

Jul. 22	WikiLeaks publishes 20,000 emails allegedly from the DNC; on the same day Guccifer 2.0 claims to have provided the documents to WikiLeaks
Oct. 7	WikiLeaks publishes 2,050 emails allegedly stolen from Clinton campaign chairman John Podesta, including excerpts from Clinton's Wall Street speeches; the dump is described as "part 1" by WikiLeaks
Oct. 10	WikiLeaks publishes "part 2" of Podesta emails
Oct. 11	WikiLeaks publishes "part 3" of Podesta emails
Oct. 12	WikiLeaks publishes "part 4" and "part 5" of Podesta emails
Oct. 13	WikiLeaks publishes "part 6" of Podesta emails
Oct. 14	WikiLeaks publishes "part 7" of Podesta emails
Oct. 15	WikiLeaks publishes "part 8" of Podesta emails, including Hillary Clinton's Goldman Sachs private paid speeches
Oct. 16	WikiLeaks publishes "part 9" of Podesta emails
Oct. 17	WikiLeaks publishes "part 10" of Podesta emails
Oct. 18	WikiLeaks publishes "part 11" of Podesta emails
Oct. 19	WikiLeaks publishes "part 12" of Podesta emails
Oct. 20	WikiLeaks publishes "part 13" of Podesta emails including emails from Barack Obama via his alleged personal email address
Oct. 21	WikiLeaks publishes "part 14" of Podesta emails
Oct. 22	WikiLeaks publishes "part 15" of Podesta emails
Oct. 23	WikiLeaks publishes "part 16" of Podesta emails
Oct. 24	WikiLeaks publishes "part 17" of Podesta emails
Oct. 25	WikiLeaks publishes "part 18" of Podesta emails
Oct. 26	WikiLeaks publishes "part 19" of Podesta emails
Oct. 27	WikiLeaks publishes "part 20" of Podesta emails
Oct. 28	WikiLeaks publishes "part 21" of Podesta emails
Oct. 29	WikiLeaks publishes "part 22" of Podesta emails

Oct. 30	WikiLeaks publishes "part 23" of Podesta emails
Oct. 31	WikiLeaks publishes "part 24" of Podesta emails; announces a "third phase" of leaks regarding US presidential election
Nov. 1	WikiLeaks publishes "part 25" of Podesta emails
Nov. 2	WikiLeaks publishes "part 26" of Podesta emails
Nov. 3	WikiLeaks publishes "part 27" of Podesta emails
Nov. 3	WikiLeaks publishes "part 28" of Podesta emails, describing them as "DOJ/FBI/Human special"
Nov. 4	WikiLeaks publishes "part 29" and "part 30" of Podesta emails
Nov. 5	WikiLeaks publishes "part 31" of Podesta emails
Nov. 6	WikiLeaks publishes "part 32" of Podesta emails
Nov. 6	WikiLeaks publishes "8,263 emails from the DNC" accompanied by the hashtag #DNCLeak2
Nov. 7	WikiLeaks publishes "part 33" and "part 34" of Podesta emails
Nov. 7	WikiLeaks claims that their "email publication servers are under a targeted DoS attack since releasing #DNCLeak2"
Dec. 1	WikiLeaks posts documents from the German Bundestag inquiry into the relationship between Germany's Bundesnachrichtendienst (BND) and the US National Security Agency (NSA)

Section 3.2: Direct Advocacy

All six of the suspected false hacktivist personas engaged in various forms of what we term Direct Advocacy: sending notifications of cyber threat activity – mainly leaks – directly to subject matter-relevant individuals or organizations that might further amplify news of that activity and bolster related political narratives. We assess that advocacy targets were strategically chosen based on their anticipated potential to maximize this dissemination, and have identified them as largely falling into the following categories:

- Journalists, particularly journalists known to cover information security topics
- Information security researchers and bloggers
- Anti-secrecy and information freedom organizations
- Genuine hacktivists and hacktivist news disseminators

- Subject matter-specific audiences relevant to the personas' claimed identities or the victims of specific incidents of threat activity

Public Twitter Advocacy

@anpoland-, Fancy Bears' Hack Team-, @pravsector-, and Bozkurt Hackers-operated Twitter accounts all directed tweets detailing their threat activity at specific individuals in the above categories. For example, on April 29, 2016, Bozkurt Hackers directed an announcement of a possible future data leak at information freedom organization Cryptome, information security reporter Kevin Collier (@KevinCollier), information security engineer and blogger Omar Benbouazza (@omarbv), and information security journalist and blogger Jeff A. Taylor (@TheFree_Lance).

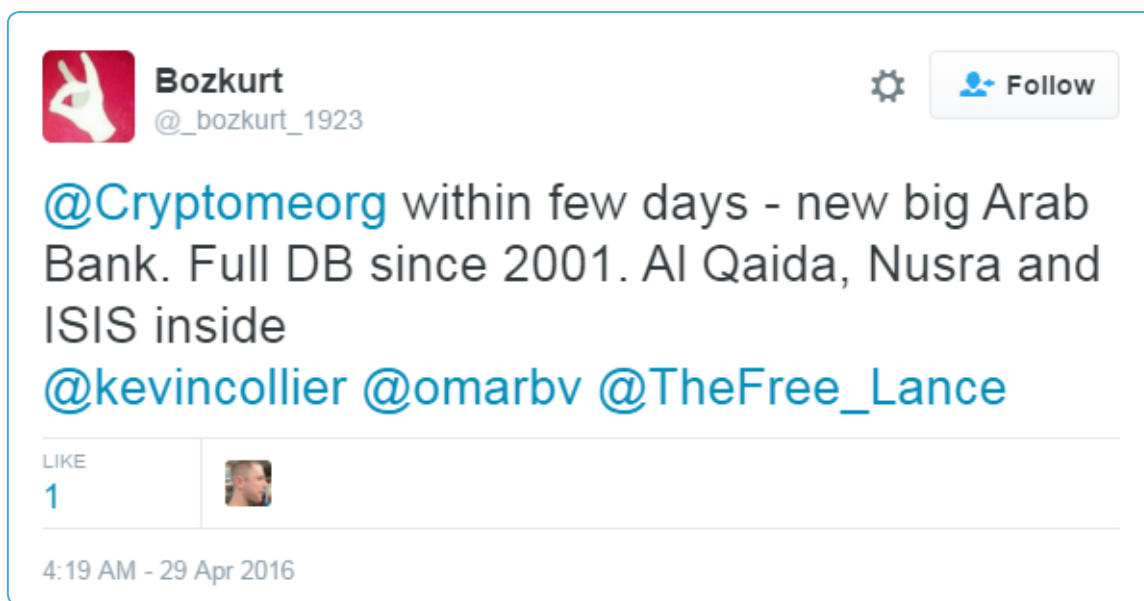


FIGURE 3.2.1: BOZKURT HACKERS ANNOUNCEMENT DIRECTED AT INFORMATION SECURITY NEWS DISSEMINATORS

In addition to information security news disseminators, we observed @pravsector and @anpoland direct tweets promoting threat activity at individuals relevant to the purported national identities of the personas and the victims of their claimed data leaks, namely Polish and Ukrainian journalists such as Marcin Dobski (@szachmad) and Sasha Vakulina (@sashavakulina).



FIGURE 3.2.2: @PRAVSECTOR AND @ANPOLAND ANNOUNCEMENTS DIRECTED AT UKRAINIAN AND POLISH JOURNALISTS, AMONG OTHER RECIPIENTS

Similarly, @anpoland and Fancy Bears' Hack Team directed tweets regarding claimed leaks of the World Anti-Doping Agency (WADA) and the Court of Arbitration for Sport (CAS) at subject matter-relevant individuals, including sports journalist Mark Fainaru-Wada (@markfwespn), nutritionist Kit Chamier (@nutritionkit), sports health author Bill Gifford (@billgifford), and health journalist Christina Stiehl (@ChristinaStiehl).

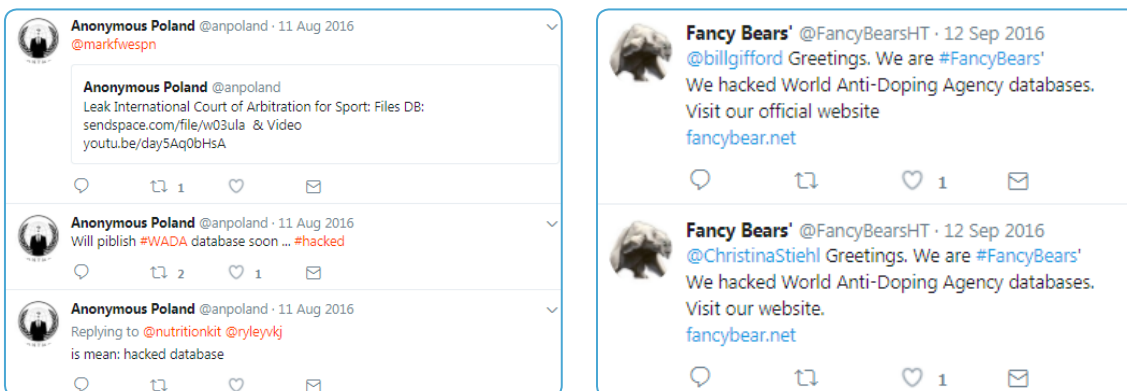


FIGURE 3.2.3: @ANPOLAND AND FANCY BEARS' HACK TEAM PROMOTE ACTIVITY TO SPORTS AND HEALTH NEWS DISSEMINATORS

As previously noted in section 1.3, @anpoland also heavily engaged in direct advocacy promoting its Bradley Foundation leak to spread the narrative of Hillary Clinton as being corrupt. This messaging was directed at various individuals including Trump campaign officials and the journalists John Pilger, Jake Tapper (CNN), Stefania Maurizi (La Repubblica), Ola Cichowlas (Moscow Times), Ian Wishart (Bloomberg), Duncan Robinson (Financial Times), Nikos Chrysoloras (Bloomberg), Ali Vitali (NBC News), Candace Smith (ABC), Bill O'Reilly (Fox News), Rebecca Ballhaus (Wall Street Journal), and George Stephanopoulos (ABC).

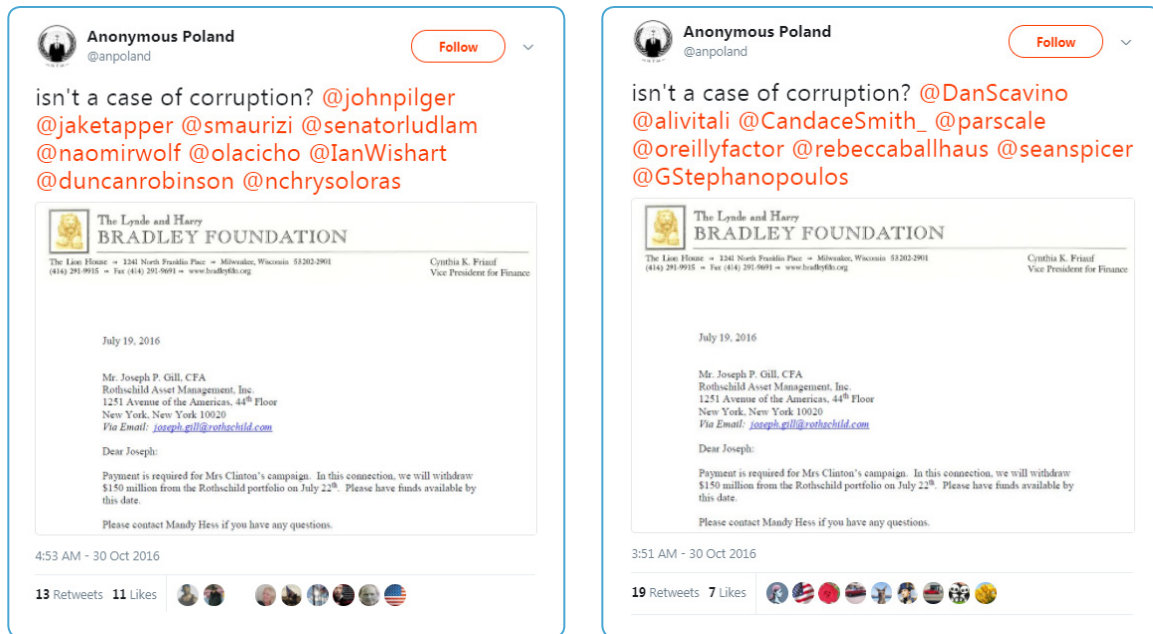


FIGURE 3.2.4: @ANPOLAND PERSONA PROMOTES A FALSIFIED LETTER TO SPECIFIC INDIVIDUALS AS PART OF ITS DIRECT ADVOCACY EFFORTS

Private Message Advocacy

Guccifer 2.0,^{79,80} DC Leaks,^{81,82} Fancy Bears' Hack Team,⁸³ and Bozkurt Hackers⁸⁴ initiated direct, private communication with journalists via email and private messaging to promote their respective data leaks. DC Leaks, Guccifer 2.0, and Fancy Bears' Hack Team also provided specific reporters with select access to purportedly leaked materials sometimes before they were made available to the public. We assess that this exclusive access was intended to further encourage selected journalists and media outlets to report on the contents of leaks by creating time-sensitive

"scoops." For example, in addition to The Hill, Guccifer 2.0 emailed documents allegedly taken from the Democratic National Committee (DNC) to journalists at Gawker and The Smoking Gun either at the same time or before releasing them publicly. The selection of these latter two publications as initial recipients of purportedly leaked DNC data again suggests the operators behind the persona possessed a particularly nuanced familiarity with US media outlets and their audiences, as these outlets have been associated with numerous high-profile, attention-generating exposés in the past.

⁷⁹ <http://www.bbc.com/news/technology-36913000>

⁸⁰ <http://www.vocativ.com/343010/guccifer-2-0-dnc-hack/>

⁸¹ <http://www.esquire.com/news-politics/a49791/russian-dnc-emails-hacked/>

⁸² <http://www.politico.com/story/2016/09/russia-hackers-clinton-campaign-state-department-228976>

⁸³ <https://arstechnica.com/security/2016/12/hackers-behind-anti-doping-leaks-please-write-about-us-well-give-you-exclusive/>

⁸⁴ <http://www.ibtimes.co.uk/hackers-behind-qatar-national-bank-set-leak-data-another-big-bank-1558120>

Section 3.3: Indirect Advocacy via Warlists

In the cases of @anpoland, Fancy Bears' Hack Team, @pravsector, and Bozkurt Hackers, we observed use of a dissemination technique that we have not previously seen employed for the promotion of genuine hacktivist threat activity: cadres of Twitter accounts, presenting themselves as unaffiliated with the personas, repetitively publishing identical tweets promoting the personas' threat activity and in some cases directly re-tweeting them or otherwise referencing their Twitter handles. We surmise that this **Indirect Advocacy** served two purposes: to further spread awareness of threat activity incidents and to boost the credibility of the personas by creating a grassroots impression that more genuine Twitter users were interested in—and talking about—these incidents than was accurate. Many of these repetitive tweets were also directed at specific journalists or other potential organic disseminators in a similar manner to that described in the Direct Advocacy section above.

The personas engaged in this indirect advocacy via use of what we have termed "**Warlists**," or systematized networks of Twitter accounts organized to promote leaks and associated political narratives in a large-scale, semi-automated fashion. While the behavior of Warlists can at times be considered a form of "astroturfing" – the practice of making a single-operator campaign appear to be grassroots – the profiles adopted by Warlist accounts often identically mimicked news organizations (both real and fabricated) instead of merely simulating grassroots, individual user activity.

We observed these Warlists publishing identical tweets at a rate too fast to be attributable to a human operator, and thus on first inspection they appear to fall into the much larger category of Twitter bots, or accounts whose activity occurs without real-time input or direction from human operators. However, we also observed these Warlists publishing content in a clearly tailored manner to promote the personas' leak activity and related narratives that suggested at least some degree of human direction. As such, Warlists better fit into the category of human-assisted bots, or "cyborg" accounts; the accounts we observed all appear to have been part of cultivated lists that produced large-scale bursts of activity following inputs from a human operator.

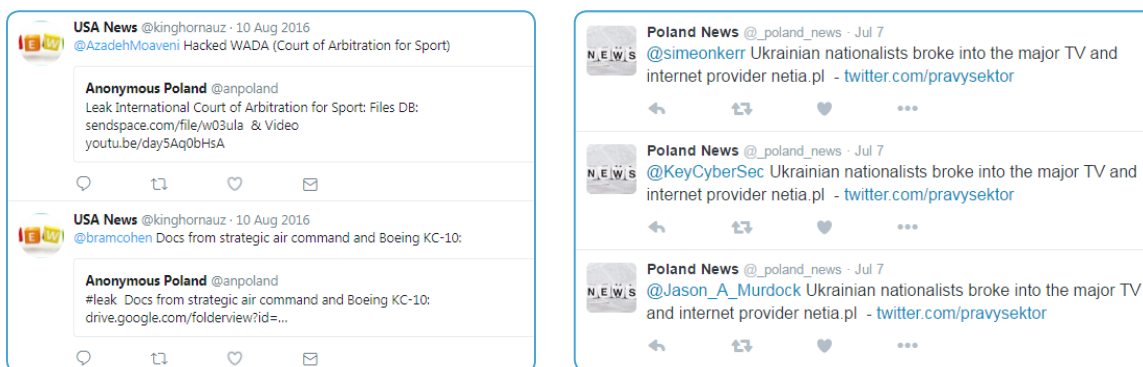


FIGURE 3.3.1: @ANPOLAND AND @PRAVSECTOR-RELATED WARLIST ACCOUNTS PRESENTING AS NEWS OUTLETS

We identify several key features of Warlists that we believe qualify them as a unique subset of bot activity:

- Warlist activity is large-scale and systematized, often with hundreds of accounts posting thousands of times in alphabetical order following a consistent schedule.
- Warlist use appears to be part of highly controlled campaigns, with content and scheduling determined beforehand by a human operator (rather than reactive to other Twitter activity)
- Warlists are regularly (though not exclusively) used to engage in indirect advocacy, promoting threat activity to pre-organized lists of specific individuals
- Warlist accounts often masquerade as independent, genuine Twitter users or news outlets
- Warlist accounts within individual lists often share identical features, such as display names and profiles
- Warlists serve political purposes rather than economic purposes such as marketing or “click” generation.

We have coined the term “Warlist” based on our observation of this technique being used to promote a #WarAgainstDemocrats campaign initiated by @anpoland on the evening of the 2016 US presidential election.

3.3.1 What are Warlists? The Example of @anpoland and the #WarAgainstDemocrats

On Nov. 8, 2016, the day of the US presidential election, @anpoland tweeted political messaging voicing opposition to the US Democratic Party, and in particular, Hillary Clinton. At 2:41 AM EST, the account tweeted: “Clinton – russian prostitute - #ClintonCorruption #Kurva #RefundPolishlandsback #WarAgainstDemocrats.” At 3:01 PM EST, the account tweeted: “#WarAgainstDemocrats – war between Republicans and Democrats – Your voice please.” Notably, @anpoland deleted both of these tweets at some point prior to Nov. 9, 2016.

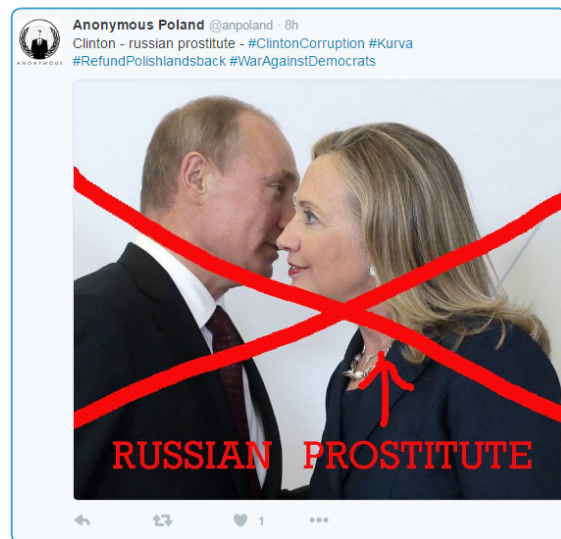


FIGURE 3.3.2: TWEET BY @ANPOLAND ON NOV. 8, 2016 USING THE HASHTAG #WARAGAINSTDEMOCRATS

The tweets received very little engagement in the form of likes or retweets; however, shortly after the second tweet, at approximately 3:20 PM EST, hundreds of other Twitter accounts started posting the single hashtag #WarAgainstDemocrats. By collecting and examining these tweets, we identified what we believe were four distinct groups of accounts (four sub-lists making up one large Warlist) tweeting the #WarAgainstDemocrats hashtag, cycling through accounts in alphabetical order by username, at a slightly fluctuating but relatively consistent rate of between 5 and 10 tweets per minute. By 7:30 PM EST, the hashtag had been pushed by the four sub-lists over 1,700 times. This activity began to taper off at around 7:30 PM, and appeared to cease entirely by 11:33 PM. Based on the data we were able to collect, at least 1,777 tweets pushed the #WarAgainstDemocrats hashtag on Nov. 8.



FIGURE 3.3.3: ANNOTATED SAMPLE OF NOV. 8, 2016 WARLIST ACTIVITY ASSOCIATED WITH @ANPOLAND. IN THIS INSTANCE, THE ACCOUNTS TWEETED ONLY THE HASHTAG #WARAGAINSTDEMOCRATS, WITH NO REFERENCE TO @ANPOLAND OR ANY CYBER THREAT ACTIVITY. NOTE THAT ALL THE ACCOUNTS HAVE DIFFERENT USERNAMES BUT SHARE ONE OF TWO DISPLAY NAMES. NOTE ALSO THAT ONE OF THESE DISPLAY NAMES WAS THE HASHTAG #RUSSIANPROSTITUTE, AGAIN A REFERENCE TO @ANPOLAND'S ORIGINAL TWEET. THE PHRASE "RUSSIAN PROSTITUTE" WAS ALSO USED BY THE PERSONA @PRAVSECTOR - A PURPORTED ADVERSARY OF @ANPOLAND.

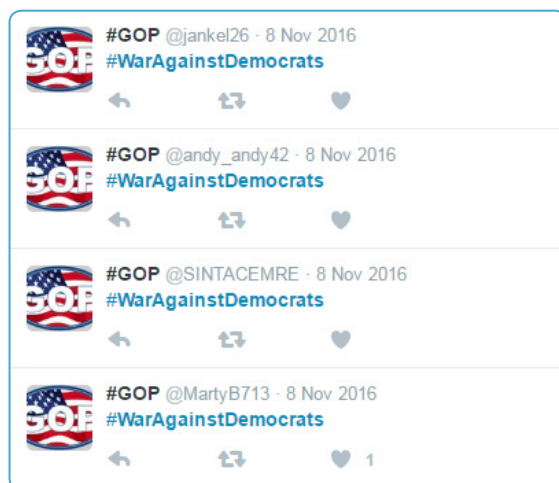


FIGURE 3.3.4: SAMPLE NOV. 8, 2016 ACTIVITY FROM A WARLIST ASSOCIATED WITH @ANPOLAND. AS HUNDREDS OF ACCOUNTS IN THESE LISTS HAVE BEEN SUSPENDED SINCE NOV. 8, THEIR CYCLICAL, ALPHABETICAL ORDERING IS NO LONGER VISIBLE VIA PUBLIC SEARCHES ON TWITTER.

While we cannot identify with certainty the specific motivation behind the Nov. 8 #WarAgainstDemocrats campaign, we believe the goal in general was to incite opposition against the Democratic Party within the US. We suspect that the operators behind @anpoland and its associated Warlist activity presumed at the time, as most observers did, that Hillary Clinton would win the election that evening, and were engaging in preliminary activity for a long-term anti-Democrat influence campaign that would continue to inflame the partisan divide among the US electorate beyond the election and undermine the expected Clinton presidency. It is also plausible that the operators hoped that the #WarAgainstDemocrats campaign might inspire non-Clinton votes in the final hours of election day; however, given the 11th hour nature of this burst of activity, we suspect this to be less likely as the primary motivation.

WARLIST SUB-LIST	FIRST ACCOUNT	LAST ACCOUNT	# ACCOUNTS IN SUB-LIST
Sub-List #1	@007Latif	@Zhuravlev1	420
Sub-List #2	@_0112635735633	@zonpig	451
Sub-List #3	@004rus	@ZuevaYa	442
Sub-List #4	@_185984043628	@zorina_e	441

FIGURE 3.3.5: SUMMARY OF THE @ANPOLAND-RELATED WARLISTS ACTIVE ON NOV. 8 AND NOV. 9, 2016.

USERNAME	TWEET	TIMESTAMP (EST)
@edanur01	#WarAgainstDemocrats	17:54
@erkan_81	#WarAgainstDemocrats	17:54
@efekinoks	#WarAgainstDemocrats	17:54
@eseantonio1	#WarAgainstDemocrats	17:54
@elyashayk	#WarAgainstDemocrats	17:54
@evreeeen4	#WarAgainstDemocrats	17:55
@emrekanbalc	#WarAgainstDemocrats	17:55
@f0rmidAbleR	#WarAgainstDemocrats	17:55
@emrullahtac	#WarAgainstDemocrats	17:55
@fedilixi	#WarAgainstDemocrats	17:55
@eneskar1	#WarAgainstDemocrats	17:55
@fedo_no	#WarAgainstDemocrats	17:55
@enginbasaran0	#WarAgainstDemocrats	17:55
@feel_the_fear	#WarAgainstDemocrats	17:56
@erere377	#WarAgainstDemocrats	17:56
@fehmifym	#WarAgainstDemocrats	17:56
@erhaner1	#WarAgainstDemocrats	17:56

FIGURE 3.3.6: SAMPLE OF ACCOUNTS FROM WARLISTS RELATED TO @ANPOLAND. ON NOV. 8, 2016, THE ACCOUNTS POSTED THE HASHTAG #WARAGAINSTDEMOCRATS AN AVERAGE OF 5-10 TIMES PER MINUTE (SHOWN HERE SLIGHTLY OUT-OF-ALPHABETICAL-ORDER DUE TO TWO SEPARATE SUB-LISTS TWEETING CONCURRENTLY, AS COLOR CODED).

On Nov. 9, 2016 at 8:28 AM EST, with the outcome of the US Presidential election having been decided, @anpoland tweeted: “#Clinton infamously lost the elections. #We #won!!! #ClintonCorruption #RotschildCorruption - #Trump #Election2016 #AmericanPeople.” Beginning at 1:15 PM EST and running until 4:37 PM EST, the same Warlist that tweeted the #WarAgainstDemocrats campaign the day prior systematically tweeted: “@[Unique User] #hacked Bradley Foundation and WON :)))” and included a copy of @anpoland’s earlier tweet. We collected data demonstrating that 4,179 unique Twitter users were recipients of this Warlist-driven indirect advocacy. The first 1,762 tweets in this run of activity misspelled “Bradley” as “Breadly” before the accounts switched to the correct spelling.



FIGURE 3.3.7: TWEET BY @ANPOLAND ON NOV. 9, 2016 THAT PRECEDED A SECOND WAVE OF WARLIST ACTIVITY

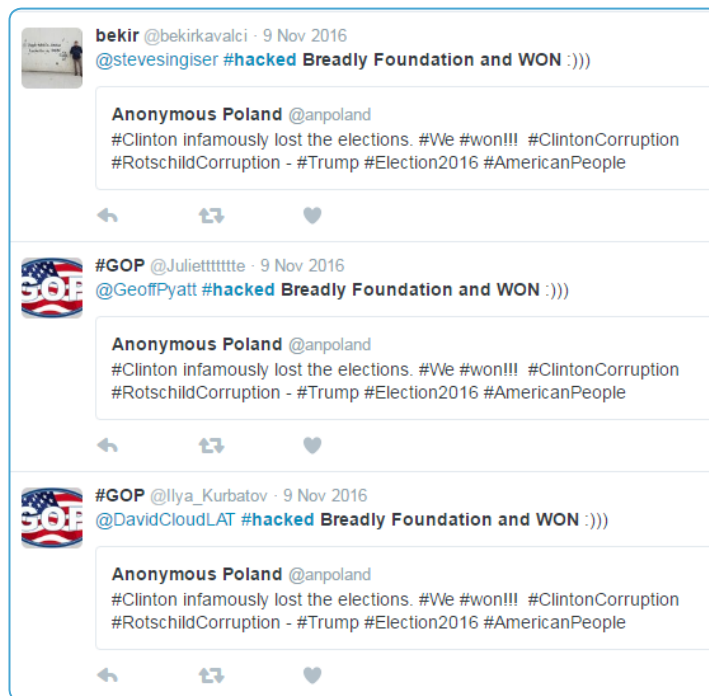


FIGURE 3.3.8: ACCOUNTS FROM @ANPOLAND-RELATED WARLIST TWEET AT AMERICAN INDIVIDUALS INVOLVED IN POLITICS OR POLITICAL JOURNALISM ON NOV. 9, 2016. THIS SCREENSHOT WAS TAKEN ON FEB. 16, 2017, AT WHICH TIME THE FIRST ACCOUNT, @BEKIRKAVALCI, HAD ALREADY SWITCHED ITS PROFILE PICTURE OVER FROM THE “GOP” PICTURE THAT ALL ACCOUNTS USED ON NOV. 9.

HAVING SEEN SIMILAR BEHAVIOR FROM SEVERAL OTHER ACCOUNTS, MOST OF WHICH WERE CREATED MORE THAN FOUR YEARS AGO, WE BELIEVE THAT THIS ACCOUNT AND OTHERS IN THIS WARLIST WERE PART OF LARGE “BUNDLES” OF TWITTER ACCOUNTS OF THE KIND THAT ARE BOUGHT AND SOLD BY GREY OR BLACK MARKET SOCIAL MEDIA ACCOUNT DEALERS.

Unlike the Nov. 8 Warlist activity, the Nov. 9 activity made specific reference to leak activity and directly associated with @anpoland by including the persona's earlier tweet. We suspect the Nov. 8 omission of references to @anpoland was deliberate and intended to trigger seemingly grassroots, un-attributable anti-Democrat political narratives. The second wave of Warlist activity also tweeted in near-alphabetical order. Additionally, we assess that the unique, legitimate Twitter users that received directed tweets from this Warlist were purposefully selected and fell into distinct categories, the most prominent being that of Hillary for America employees. When the tweets are arranged chronologically, the following groups of recipients quickly become evident:

- World leaders
- Ministries of Foreign Affairs
- US Department of State accounts
- Various U.S. federal government employees and organizations
- Members of the US Congress
- Journalists from a variety of countries, mainly based in the US
- US-based celebrities (specifically likely Clinton supporters)
- Hillary for America employees and activists
- New Hampshire political activists, individuals, and organizations
- Indiana political activists, individuals, and organizations
- Virginia individuals and organizations

USERNAME	TWEET	GROUP	TIMESTAMP (EST)
@Nikolaev0076	@HillaryforKY hacked Bradley Foundation and WON :)))	Hillary for America (by US state)	16:10:01
@NinaSudenkova	@momoftwoxy hacked Bradley Foundation and WON :)))	User from Indiana	16:10:01
@Nikolay_71_	@HillaryforIN hacked Bradley Foundation and WON :)))	Hillary for America (by US state)	16:10:02
@Nobody_anywhere	@Heritage hacked Bradley Foundation and WON :)))	Political conservative think-tank	16:10:02
@Nikolja7777	@HillaryforMD hacked Bradley Foundation and WON :)))	Hillary for America (by US state)	16:10:04
@Nubjara	@dicklugar hacked Bradley Foundation and WON :)))	Politically conservative senator from Indiana	16:10:04
@NipeIII	@HillaryforMA hacked Bradley Foundation and WON :)))	Hillary for America (by US state)	16:10:05
@Nz456	@MarchantforTX24 hacked Bradley Foundation and WON :)))	Politically conservative user	16:10:05
@OH_Rino	@Kevin_B_Allen hacked Bradley Foundation and WON :)))	Politically conservative user	16:10:06
@No_Yulia_	@HillaryforMO hacked Bradley Foundation and WON :)))	Hillary for America (by US state)	16:10:07
@Nurdaulet94	@HillaryforNJ hacked Bradley Foundation and WON :)))	Hillary for America (by US state)	16:10:08
@OLKA69	@MatthewSwiontek hacked Bradley Foundation and WON :)))	User from Indiana	16:10:08

FIGURE 3.3.9: SAMPLE TWEETS FROM TWO SUB-LISTS OF AN @ANPOLAND-RELATED WARLIST (COLOR CODED) DIRECTING TWEETS AT LEGITIMATE TWITTER USERS

3.3.2 Overview of Identified Warlist Activity and Aims

We have identified 25 separate incidents of Warlists being used to promote threat activity or politicized narratives on behalf of @anpoland, @pravsector, Fancy Bears' Hack Team, and Bozkurt Hackers. Among the four personas, we observed the largest Warlists being employed by @anpoland to support indirect advocacy of its data leaks. In almost every instance of Warlist activity, the accounts within each list shared identical display names, and in one case, we observed the same profile picture and display name – “China Daily” – being used for all accounts in two distinct Warlists used by @pravsector and @anpoland respectively. Although the specific accounts that constituted each of the two Warlists differed, the use of identical display features between them provides an additional indicator that the @pravsector and @anpoland personas, which presented as adversarial towards each other, were controlled by the same operator(s).

The following table provides summary details for each of the incidents of Warlist activity we identified. We strongly suspect that other occurrences of Warlist usage beyond those discussed here have gone unnoticed by us and other observers.



WARLISTS
used to promote
THREAT
ACTIVITY

WARLIST ACCOUNT SHARED DISPLAY NAME(S)	PURPOSE	DATES OF OPERATION	RELATED PERSONA	IDENTIFIED NUMBER OF UNIQUE ACCOUNTS IN WARLIST(S)	NUMBER OF UNIQUE INDIRECT ADVOCACY RECIPIENTS
#GOP - WON	Promoted #WarAgainstDemocrats and @anpoland's attack on Bradley Foundation	11/8-9/2016	@anpoland	1,754	4,179
#ClintonCorruption / #ClintonCorruption	Promoted @anpoland's attack on Bradley Foundation	11/2-3/2016	@anpoland	1,008	8,254
Breaking News	Promoted @anpoland's attack on Bradley Foundation	11/1/2016	@anpoland	890	3,574
News	Promoted @anpoland's attack on Bradley Foundation	10/31/2016	@anpoland	132	494
Question	Promoted @anpoland's attack on Bradley Foundation	10/31/16	@anpoland	428	1628
[Not identical - used Fox News and Sky News iconography]	Promoted @anpoland's attack on Bradley Foundation	10/30/2016	@anpoland	3	34
Anti-Global	Promoted @anpoland's attack on Bradley Foundation	10/29-11/1/2016	@anpoland	285	2,321
[Not identical]	Promoted Fancy Bears' Hack Team's attack on WADA	9/12-13/2016	Fancy Bears' Hack Team	3	65
USA News	Promoted @anpoland's attack on WADA, the Court of Arbitration for Sport, and (purportedly) Boeing	8/10-11/2016	@anpoland	193	1,249
News	Promoted @anpoland's attack on the Court of Arbitration for Sport	8/10/2016	@anpoland	288	2,795
China Daily	Promoted @anpoland's attack on the Court of Arbitration for Sport	8/10/2016	@anpoland	81	799
EuroPress	Promoted @pravsector's attack on the Central Ohio Urology Clinic	8/2/2016	@pravsector	192	2,036
China Daily	Promoted @pravsector's attack on the Central Ohio Urology Clinic	8/2/2016	@pravsector	146	1,340
IT News	Promoted @pravsector's attack on the Central Ohio Urology Clinic	8/1-2/2016	@pravsector	95	799
News	Promoted @anpoland's purported leak of files from the Ukrainian Government	8/1/2016	@anpoland	123	1,514
Ukraine.info / Ukr-info	Promoted @pravsector's attack on Armenian Embassy in Ukraine	7/21-8/1/2016	@pravsector	50	2,817
Poland News	Promoted @pravsector's attack on Netia	7/7/2016	@pravsector	1	45
Lemberg	Promoted @pravsector's attack on Netia	7/7-8/2016	@pravsector	99	4,406
Al Jazeera	Promoted Bozkurt Hackers' attack on Qatar National Bank	5/1-2/2016	Bozkurt Hackers	17	332
Qatar Air	Promoted Bozkurt Hackers' attack on Qatar National Bank	5/1-2/2016	Bozkurt Hackers	23	446
QNB	Promoted Bozkurt Hackers' attack on Qatar National Bank	5/1-2/2016	Bozkurt Hackers	24	425

AntiQatar	Promoted Bozkurt Hackers' attack on Qatar National Bank	4/24-25/2016	Bozkurt Hackers	11	231
Anti-Bank	Promoted Bozkurt Hackers' attack on Qatar National Bank	4/22-23/2016	Bozkurt Hackers	4	310
Arab News	Promoted Bozkurt Hackers' attack on Qatar National Bank	4/22-23/2016	Bozkurt Hackers	4	200
AntiQNB	Promoted Bozkurt Hackers' attack on Qatar National Bank	4/21-22/2016	Bozkurt Hackers	4	0

FIGURE 3.3.10: SUMMARY DETAILS FOR 25 SEPARATE OBSERVED INCIDENTS OF WARLIST ACTIVITY BY FOUR PERSONAS (PRESENTED IN REVERSE CHRONOLOGY)

Collectively, two main aims appear to have driven the use of Warlists by the @anpoland, @pravsector, Fancy Bears' Hack Team, and Bozkurt Hackers personas: cyber threat activity promotion and political narrative promotion.

Cyber Threat Activity Promotion

The primary use of Warlists appears to have been to promote and draw large-scale attention to the personas' cyber threat activity. In particular, we surmise that Warlists were deployed when a target or activity was not considered sensational enough on its own to garner organic attention from third parties. For example:

- As detailed above, we observed Warlists being used to promote @anpoland's claimed DDoS attacks and data leaks targeting the Bradley Foundation in October and November 2016. @anpoland and its associated Warlists vaguely claimed that the allegedly leaked data demonstrated corruption on the part of the Clinton campaign; these claims failed to solidify into significant or demonstrable allegations. The Bradley Foundation is not a well-known organization, tends to support politically conservative causes and was therefore unlikely to support Clinton, and with the activity targeting the organization occurring during the height of election season, coverage had to compete with other, higher-profile news.
- We observed Warlists being used to promote @pravsector's claimed leaks of data from the Armenian Embassy in Ukraine and Polish telecom Netia in July 2016. The claimed leak from the Armenian Embassy does not appear to have generated any international attention. While @pravsector's data leaks from the Polish Ministry of Defense and Netia were reported

by international news outlets, the use of Warlists to promote the Netia leak may suggest that @pravsector did not anticipate it would generate any significant media coverage beforehand.

- On April 21, 2016, we observed a Warlist being used to promote Bozkurt Hackers' claimed data leak from Qatar National Bank (QNB), which the persona first announced on April 20, 2016. The leak was not widely reported by international news outlets until April 25, 2016.



FIGURE 3.3.11: BOZKURT HACKERS-ASSOCIATED WARLIST ACTIVITY WITH THE IDENTICAL DISPLAY NAME "ANTIQNB" PROMOTES THE HASHTAG #BOZKURTHACKERS AND AN ARTICLE DESCRIBING THE QNB DATA LEAK ON APRIL 21, 2016. NOTE THE DIFFERENT ACCOUNT NAMES ALL EMPLOYING VARIATIONS OF "ANTIQNB" AS WELL.

Political Narrative Promotion

Based on their close association with the four personas in question, and their near-exclusive focus on threat activity claims, we assess that cyber threat activity promotion was the primary purpose for the deployment of Warlists. However, some Warlists also promoted politically partisan hashtags, including, in at least one instance, #WarAgainstDemocrats, a narrative absent of any reference to cyber threat activity. We believe that the promotion of political narratives, including narratives that closely resemble those pushed by the more carefully cultivated and in some cases less automated social media “trolls” that we also suspect served Russian political interests, suggests the presence of a large, sophisticated, and complex information operations machinery at work.

“Trending Topics” Manipulation

In the case of both cyber threat activity promotion and political narrative promotion, we assess that Warlists were designed to take advantage of Twitter’s “Trending Topics” algorithm. Large, automated networks of Twitter accounts have often been used in the past to manipulate Twitter’s “Trending Topics” algorithm, which populates a “Trending Topics” sidebar and thereby exposes desired themes to a wider audience than would be practical via

one-to-one sharing between individual users. The exact number of unique user-created tweets sharing an identical phrase or hashtag required to trigger this algorithm is not publicly known, but estimates range from roughly 400 to 1,500 tweets, with factors such as time of day and “originality” also playing a role.

We suspect that Warlists were similarly intentionally designed to artificially trigger Twitter’s “Trending Topics” algorithm, in order to expose certain hashtags or phrases to wide audiences.

- @recentideas is an automated Twitter account that generates random tweets based on machine learning, and appears to populate parts of its tweets based on trending hashtags or phrases. On Aug. 10, 2016, at 11:14 PM EST, the account posted “#HACKED #WADA #NEWS #BREAKING” as part of an otherwise incoherent message. Earlier that day, an @anpoland-associated Warlist used this exact language in its promotion of @anpoland’s claimed leak of data from WADA and the Court of Arbitration for Sport (CAS). We are almost certain that the volume of this Warlist’s activity was large enough to trigger the appropriation of this language by @recentideas.

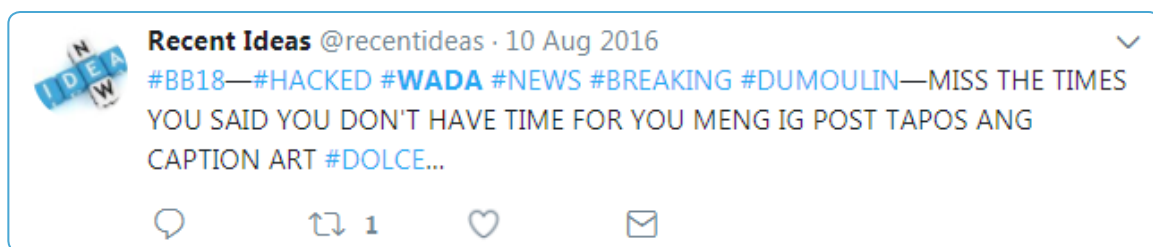


FIGURE 3.3.12: THE AUTOMATED TWITTER ACCOUNT @RECENTIDEAS TWEETS MESSAGING THAT CORRESPONDS TO @ANPOLAND THREAT ACTIVITY ON AUG. 10, 2016. THIS MESSAGE WAS ALMOST CERTAINLY POPULATED BASED ON ACTIVITY FROM AN @ANPOLAND-ASSOCIATED WARLIST IN WHICH ACCOUNTS MASQUERADED AS A MEDIA OUTLET NAMED “USA NEWS.”

- #HillaryDown was promoted by an @anpoland-associated Warlist (Anti-Global) on Oct. 29, 2016, along with messaging regarding @anpoland's purported compromise of the Bradley Foundation. The #HillaryDown hashtag was flagged as "trending" by the account @TrendsRio, one of a number of Twitter accounts that monitor hashtag trending in different areas of the world. @TrendsRio flagged this as a trending hashtag at 10:52PM EST. Our collection of tweet data for that date reveals that the @anpoland-associated Warlist accounts had posted the hashtag dozens of times within an hour prior to it being flagged by @TrendsRio.
- #WarAgainstDemocrats was shared by an @anpoland-associated Warlist with no additional messaging making reference to any cyber threat activity. Accounts tweeted at a rate of approximately 400-500 tweets per hour, which is in the low but still plausible range for triggering Twitter's "Trending Topics" algorithm. As noted previously, the hashtag was shared by the four sub-lists over 1,750 times over roughly 5 hours.

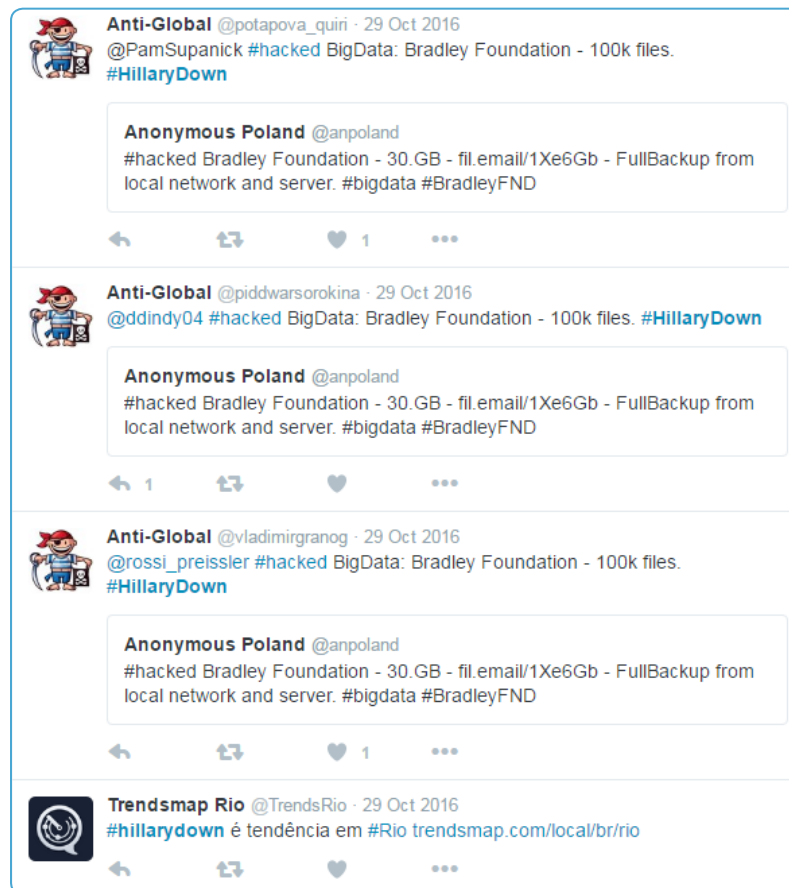


FIGURE 3.3.13: @TRENDSRIO RECORDS #HILLARYDOWN AS TRENDING IN THE MIDST OF THE HASHTAG'S PROMOTION BY AN @ANPOLAND-ASSOCIATED WARLIST. A TWITTER SEARCH FOR #HILLARYDOWN DOES NOT DISPLAY THE DOZENS OF MENTIONS OF THIS HASHTAG BY THIS WARLIST PRIOR TO IT BEING FLAGGED BY @TRENDSRIO, ALTHOUGH INDIVIDUAL SEARCHES OF ACTIVITY FOR MEMBERS OF THE WARLIST WILL RETURN THIS DATA.

Distinct Warlists Directing Messaging at Identical Recipients

We observed numerous overlaps in the sets of recipients targeted with directed tweets by Warlists promoting the activities of @anpoland, Fancy Bears' Hack Team, @pravsector, and Bozkurt Hackers. That is, Warlists associated with these four purportedly distinct personas frequently directed tweets at identical accounts, with the overlaps between @anpoland's and @pravsector's targeted audiences being so extensive as to make those audiences appear almost identical. Figures 3.3.14 and 3.3.15 below

illustrate these overlaps in target audiences between the four personas. One particularly revealing insight from Figure 3.3.14 is the heavy emphasis the personas placed on pushing messaging to mainstream media-affiliated accounts and accounts known to disseminate hacktivist-related news content, providing further evidence that the operator(s) behind the personas may have strategically selected advocacy recipients based on those accounts' anticipated potential to maximize further dissemination and amplification of threat activity announcements and related political narratives.

RECIPIENT ACCOUNT	BOZKURT HACKERS WARLISTS	@PRAVSECTOR WARLISTS	@ANPOLAND WARLISTS	FANCY BEARS' HACK TEAM WARLISTS
@aavst				
@ABC				
@AFP				
@anonops				
@AnonPress				
@AnonyOps				
@AP				
@attackerman				
@bartongellman				
@BBCBreaking				
@BreakingNews				
@CNN				
@cnnbrk				
@Cryptomeorg				
@EHackerNews				
@erinmcunningham				
@FoxNews				
@FRANCE24				
@ggreenwald				
@HackRead				
@J_Bloodworth				
@Jack_Hanrahan				

@jamesrbuk				
@jeremyscahill				
@JM_Beck				
@joshua_landis				
@LizSly				
@MailOnline				
@michaeldweiss				
@mikkosniemela				
@montie				
@NSAGov				
@nypost				
@nytimes				
@RaniaKhalek				
@realDonaldTrump				
@Reuters				
@RT_com				
@ruskin147				
@ShippersUnbound				
@SkyNews				
@StateDept				
@stuartmillar159				
@tarangoNYT				
@tedcruz				
@Telegraph				
@thegarance				
@TheHackersNews				
@wellsia				
@WhiteHouse				
@wikileaks				
@YourAnonNews				

FIGURE 3.3.14: ACCOUNTS RECEIVING DIRECTED MESSAGES FROM DISTINCT WARLISTS ASSOCIATED WITH THREE OR MORE PERSONAS

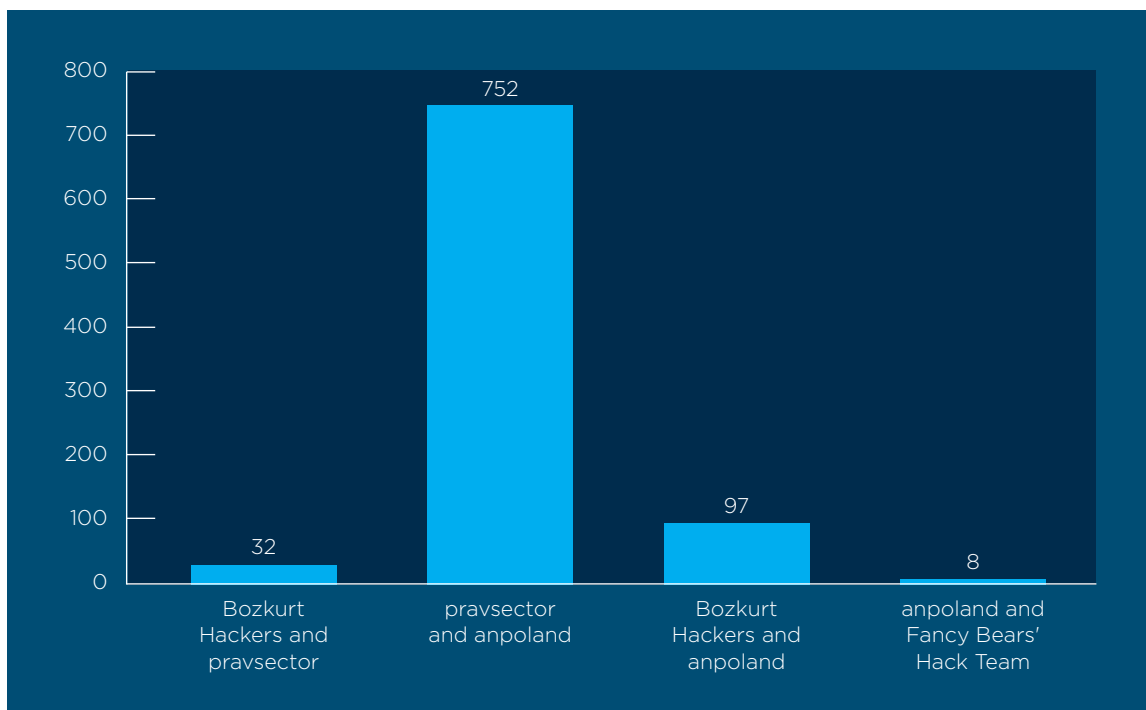


FIGURE 3.3.15: VOLUMES OF TARGETED RECIPIENT ACCOUNTS SHARED BY WARLISTS ASSOCIATED WITH TWO PERSONAS. NOTE THE HIGH NUMBER OF RECIPIENT ACCOUNTS SHARED BETWEEN WARLISTS ASSOCIATED WITH @PRAVSECTOR AND @ANPOLAND

Warlist Accounts Masquerading as Journalistic News Entities

One notable feature of some Warlists was the attempt to portray their constituent accounts as representing legitimate news outlets, itself an adoption of their own element of brand appropriation, seemingly to nurture the image of credibility, to obscure their true nature, and perhaps to also instill perceptions of newsworthiness in a ploy to motivate mainstream media coverage. For example, following @anpoland's Oct. 29, 2016 Bradley Foundation leak announcement, Warlist accounts engaging in indirect advocacy of the leak attempted to present themselves as affiliated with Sky News and Fox News through the use of branded profile pictures (See Figure 3.3.16). Additionally, many entire Warlists adopted news-related identities, with some adopting the names of genuine media entities (China Daily, Al Jazeera, Arab News) and others appearing to have either invented new brands or otherwise presented as news outlets ("Breaking News," "News," "IT News," "USA News," "EuroPress," "Poland News").

In a separate manifestation of indirect advocacy, Warlist accounts promoting @pravsector's leak from the Armenian Embassy in Ukraine attempted to portray themselves as independent, potentially partisan purveyors of Ukrainian news, using the identical display name "Ukraine.info" (See Figure 3.3.17).



FIGURE 3.3.16: @ANPOLAND-RELATED WARLIST ACCOUNTS DUBIOUSLY PRESENT THEMSELVES AS AFFILIATED WITH SKY NEWS AND FOX NEWS, AS THEY NOTIFY THE REUTERS ACCOUNTS @REUTERSINDIA AND @TAXWATCH, AND BLOOMBERG REPORTER SEBASTIAN TONG (@SEBBYTONG), OF THE OCT. 29, 2016 BRADLEY FOUNDATION LEAK.

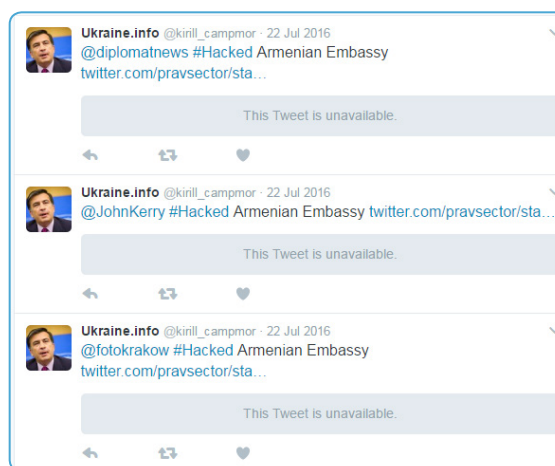


FIGURE 3.3.17: WARLIST ACCOUNTS LINKED TO @PRAVSECTOR PROMOTE THREAT ACTIVITY TARGETING THE ARMENIAN EMBASSY IN UKRAINE

3.3.3: Warlist Account Characteristics

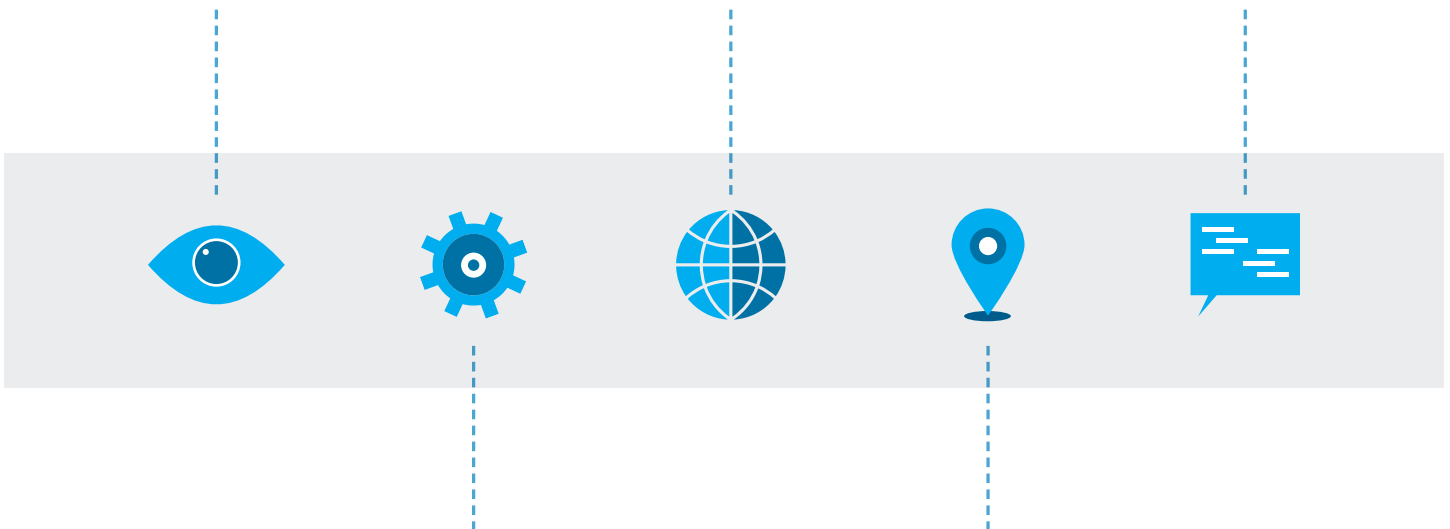
Since the majority of Warlist accounts we observed have since been suspended by Twitter, and since the activity of many accounts is filtered and therefore not visible in Twitter searches, Warlist activity related to the four personas is no longer easy to discover in most cases. Warlist accounts possess several unique characteristics, however, that can aid in their identification:

- Warlist activity is systematized (alphabetical, scheduled)
- Accounts within individual Warlists almost always share identical or similar profile features:
 - Identical display names and/or profile pictures
 - Identical descriptions
 - Identical locations
 - Identically sourced locations
- Accounts tweet identical or very similar content
- Accounts often masquerade as independent, genuine users or news outlets (as discussed briefly above)
- Warlists regularly engage in indirect advocacy, and as such:
 - Promote threat activity
 - Systematically send directed messages on a large scale to individuals in various fields based on pre-organized lists

Account activity is systematized (alphabetical, scheduled)

A striking aspect of Warlist activity is the deployment of accounts in a scheduled and alphabetized way. The Warlists we recorded were all deployed to create bursts of Twitter activity either promoting threat activity by personas (i.e. indirect advocacy) or to promote partisan/political narratives. These bursts can be linked to specific persona tweets based on threat claims or hashtag usage. While the bursts of Warlist activity clearly occurred in response to individual persona tweets, the time lapse between original tweet and Warlist activity for different Warlists was not identical, suggesting that some degree of human direction may have determined when Warlist activity would begin.

We observed several Warlists tweeting content in alphabetical order by account name, demonstrating their systematized nature. For activity that occurred between April and November 2016, most Warlists no longer exist on Twitter in either their complete form or at all, making it impossible to view alphabetization via public Twitter searches.



USERNAME	DISPLAY NAME	TWEET	TIMESTAMP (EST)
@antiqatar_9	AntiQatar	@BenjaminKweskin PLS RT #StupedThani #Qatarbank was hacked. Link for Archive pin on my top.	6:59:26
@antiqatar_7	AntiQatar	@GeordieStory PLS RT #StupedThani #Qatarbank was hacked. Link for Archive pin on my top.	6:59:27
@antiqatar_6	AntiQatar	@hansmollman PLS RT #StupedThani #Qatarbank was hacked. Link for Archive pin on my top.	6:59:29
@antiqatar_5	AntiQatar	@MichaelPDeacon PLS RT #StupedThani #Qatarbank was hacked. Link for Archive pin on my top.	6:59:30
@antiqatar_4	AntiQatar	@reportedly PLS RT #StupedThani #Qatarbank was hacked. Link for Archive pin on my top.	6:59:31
@antiqatar_3	AntiQatar	@Nick_Ashdown PLS RT #StupedThani #Qatarbank was hacked. Link for Archive pin on my top.	6:59:33
@antiqatar_2	AntiQatar	@SarkawtShams PLS RT #StupedThani #Qatarbank was hacked. Link for Archive pin on my top.	6:59:34

FIGURE 3.3.18: SAMPLE ACCOUNTS IN THE “ANTIQATAR” WARLIST PROMOTING THREAT ACTIVITY BY BOZKURT HACKERS, TWEETING IN REVERSE NUMERICAL ORDER ON APRIL 25, 2016

USERNAME	DISPLAY NAME	TWEET	TIMESTAMP (EST)
@84rjabova	Ukraine. info	@MSF More 600mb armenian files [link to download]	12:14:10
@burnnul_alena	Ukraine. info	@FarukYaman44 More 600mb armenian files [link to download]	12:14:59
@judina_opdo1983	Ukraine. info	@thedailybeast More 600mb armenian files [link to download]	12:15:23
@korjakinafuddlo	Ukraine. info	@LeadershipQtss More 600mb armenian files [link to download]	12:16:01
@majinskristina	Ukraine. info	@NBCNews More 600mb armenian files [link to download]	12:16:13
@nadezhda_todua	Ukraine. info	@TemiaBrinson More 600mb armenian files [link to download]	12:16:38

FIGURE 3.3.19: SAMPLE ACCOUNTS IN THE “UKRAINE.INFO” WARLIST PROMOTING THREAT ACTIVITY BY @PRAXSECTOR, TWEETING IN ALPHABETICAL ORDER ON JULY 21, 2016

USERNAME	DISPLAY NAME	TWEET	TIMESTAMP (EST)
@Andrew88887777	Breaking News	@FredBThird Hacked Big Foundation #Rothschilds - 100k files - [link to @anpoland status]	5:42
@BarbaAdams	Breaking News	@TheFix Hacked Big Foundation #Rothschilds - 100k files - [link to @anpoland status]	5:43
@CharvisF	Breaking News	@HuntsmanAbby Hacked Big Foundation #Rothschilds - 100k files - [link to @anpoland status]	5:45
@CloseToDeath_	Breaking News	@niniofetalvo Hacked Big Foundation #Rothschilds - 100k files - [link to @anpoland status]	5:45
@CuteTokenmfc	Breaking News	@DennisDMZ Hacked Big Foundation #Rothschilds - 100k files - [link to @anpoland status]	5:45
@DaMacdonough	Breaking News	@tarasproduction Hacked Big Foundation #Rothschilds - 100k files - [link to @anpoland status]	5:45
@LOvelieBOnes	Breaking News	@BreitbartNews Hacked Big Foundation #Rothschilds - 100k files - [link to @anpoland status]	5:51
@OnDatt305	Breaking News	@Mosheh Hacked Big Foundation #Rothschilds - 100k files - [link to @anpoland status]	5:54
@Per_Nilsson_	Breaking News	@VictoriaRColey Hacked Big Foundation #Rothschilds - 100k files - [link to @anpoland status]	5:55
@QuotesITweet	Breaking News	@ron_fournier Hacked Big Foundation #Rothschilds - 100k files - [link to @anpoland status]	5:55
@StefFranco	Breaking News	@VincentHarris Hacked Big Foundation #Rothschilds - 100k files - [link to @anpoland status]	5:57
@Zane412	Breaking News	@AmyArgetsinger Hacked Big Foundation #Rothschilds - 100k files - [link to @anpoland status]	5:58
@asdfghjkle	Breaking News	@GingerGibson Hacked Big Foundation #Rothschilds - 100k files - [link to @anpoland status]	6:00
@discipline_24_7	Breaking News	@petesnyder Hacked Big Foundation #Rothschilds - 100k files - [link to @anpoland status]	6:04
@luqmanqadir	Breaking News	@examinerpolitic Hacked Big Foundation #Rothschilds - 100k files - [link to @anpoland status]	6:11

FIGURE 3.3.20: SAMPLE ACCOUNTS IN THE “BREAKING NEWS” WARLIST PROMOTING THREAT ACTIVITY BY @ANPOLAND, TWEETING IN ALPHABETICAL ORDER ON NOV. 1, 2016. NOTE THAT IN THIS CASE MULTIPLE ALPHABETIZED LISTS ARE STACKED TOGETHER, SUGGESTING THAT THE FULL WARLIST IS AN AMALGAMATION OF SMALLER SUBLISTS.

USERNAME	TWEET	TIMESTAMP (EST)
@askabik816	@HackedCom #WADA databases leaked. Team USA take doping. Athletes Medical files revealed [link to download]	4:50:18
@askabik816	@FreedomHackerr #WADA databases leaked. US Team takes doping. Athletes Medical files revealed [link to download]	4:54:06
@askabik816	@HSIndia #WADA databases leaked. Team USA takes doping. Athletes Medical files revealed [link to download]	5:03:35
@askabik816	@LeakedSource #WADA databases leaked. Team USA takes doping. Athletes Medical files revealed [link to download]	7:26:57
@jednikiva	@ANONIMUS3000 Download hacked #WADA databases databases at website [link to download]	8:16:01
@jednikiva	@lowbobgaming Download hacked #WADA databases databases at website [link to download]	8:17:01
@jednikiva	@anonymus1_2 Download hacked #WADA databases databases at website [link to download]	8:17:18
@jednikiva	@ThaRealANONIMUS Download hacked #WADA databases databases at website [link to download]	8:17:40
@jednikiva	@DUDUSMILETIME Download hacked #WADA databases databases at website [link to download]	8:17:56
@otigtunt	@wada_ama Download #WADA databases at website [link to download]	8:34:11
@otigtunt	@wada_ama Download #WADA databases at website [link to download]	8:34:24
@otigtunt	@wada_ama @IBSFsliding Download #WADA databases at website [link to download]	8:34:44

FIGURE 3.3.21: SAMPLE ACCOUNTS IN A WARLIST THAT PROMOTED THREAT ACTIVITY BY FANCY BEARS' HACK TEAM, TWEETING IN ALPHABETICAL ORDER ON SEP. 13, 2016.

Accounts Share Identical or Similar Profile Features

One consistent characteristic of Warlist accounts was their use of identical, campaign-specific profile features, including display names, profile pictures, and profile descriptions. Additionally, we observed groups of accounts draw their stated locations from what appear to be identical sources. We believe that Warlist accounts are most likely assigned identical features to efficiently make them appear to be legitimate Twitter users. In some cases, identical characteristics among accounts may also be used to promote a specific campaign message itself (for example, the common use of #ClintonCorruption as a display name as illustrated below).

IDENTICAL DISPLAY NAMES AND/OR PROFILE PICTURES

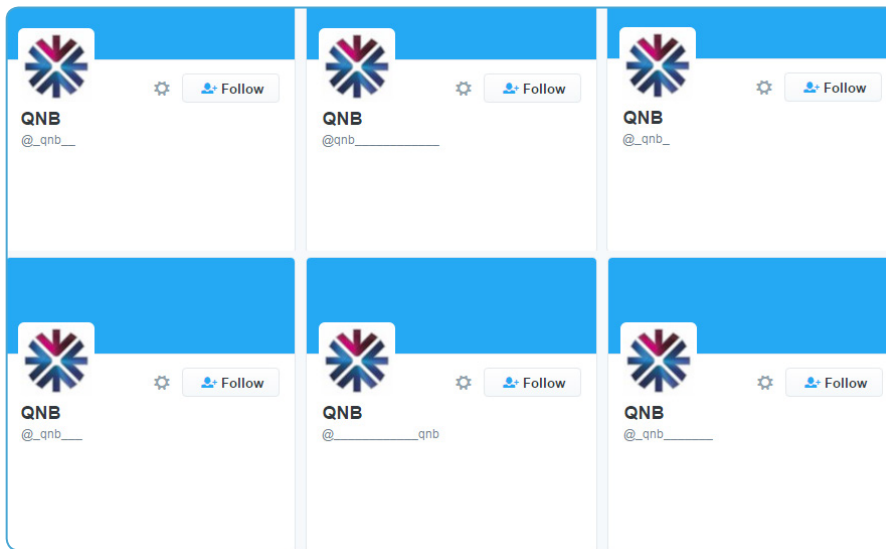


FIGURE 3.3.22: SAMPLE WARLIST ACCOUNTS THAT PROMOTED THREAT ACTIVITY BY BOZKURT HACKERS. ALL SHARE THE SAME DISPLAY NAME AND PROFILE PICTURE.

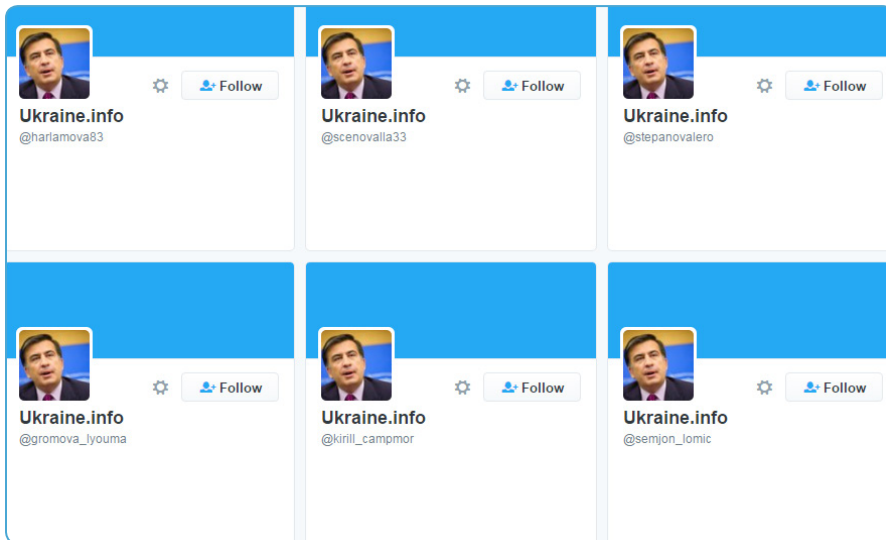


FIGURE 3.3.23: SAMPLE WARLIST ACCOUNTS THAT PROMOTED THREAT ACTIVITY BY @PRAVSECTOR. ALL ACCOUNTS USED A PICTURE OF MIKHEIL SAAKASHVILI, A FORMER UKRAINIAN GOVERNOR WHO ACTIVELY OPPOSES RUSSIAN PRESIDENT VLADIMIR PUTIN AND IS CRITICAL OF UKRAINIAN PRESIDENT PETRO POROSHENKO.

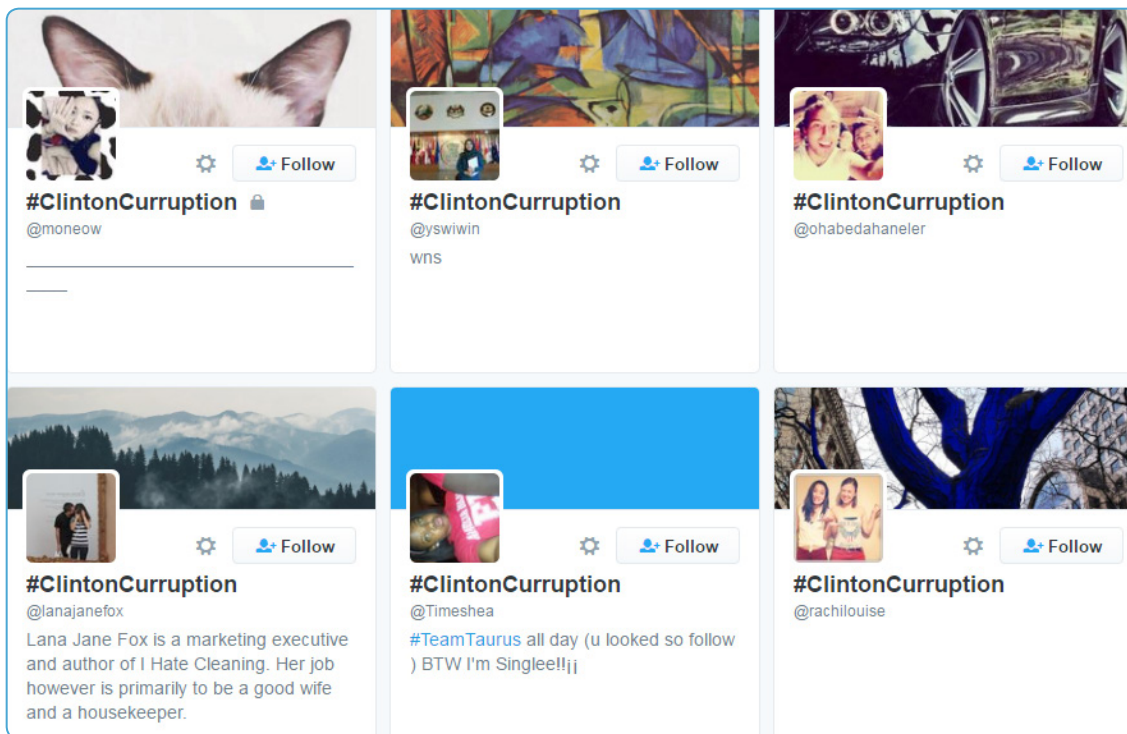


FIGURE 3.3.24: SAMPLE WARLIST ACCOUNTS THAT PROMOTED THREAT ACTIVITY BY @ANPOLAND, WHICH ALL USED THE INCORRECTLY SPELLED #CLINTONCURREPTION HASHTAG AS A DISPLAY NAME. A SEPARATE NETWORK OF ACCOUNTS USED THE CORRECTLY SPELLED #CLINTONCORRUPTION.

IDENTICAL DESCRIPTIONS / LOCATIONS



FIGURE 3.3.25: ACCOUNTS BELONGING TO THE “ANTI-GLOBAL” WARLIST, WHICH PROMOTED THREAT ACTIVITY BY @ANPOLAND. THESE ACCOUNTS FEATURED THE IDENTICAL LOCATION “RIO.”



FIGURE 3.3.26: ACCOUNTS BELONGING TO THE @ANPOLAND-ASSOCIATED “#GOP – WON” WARLIST, WHICH PROMOTED THE PARTISAN HASHTAG #WARAGAINSTDEMOCRATS. THESE ACCOUNTS SHARED AN IDENTICAL DESCRIPTION, “#WON,” WHICH THEY DISPLAYED ON NOV. 9, 2016. THE ACCOUNTS ALSO SHARED THE IDENTICAL LOCATION “DOTCOM.”

IDENTICALLY SOURCED LOCATIONS

USERNAME	DISPLAY NAME	LOCATION
roeschab	EuroPress	Hobucken
religionpne	EuroPress	Cataldo
rattlebraing	EuroPress	Thacker
rainsnu	EuroPress	Fortseneca
radixyx	EuroPress	Absarokee
quotabk	EuroPress	Mulkeytown
quitxu	EuroPress	Breauxbridge
puissancey	EuroPress	Gusher
publiusrz	EuroPress	Cedarmountain
profilejj	EuroPress	Lamirada
procliticq	EuroPress	Nikep
presidencyy	EuroPress	Canoncity
prescribeazu	EuroPress	Northtruro

FIGURE 3.3.27: ACCOUNTS BELONGING TO THE “EUROPRESS” WARLIST, WHICH PROMOTED THREAT ACTIVITY FOR @PRAVSECTOR. THE ACCOUNT “BIO” SECTIONS FEATURE THE NAMES OF SMALL US TOWNS OR CITIES. WE BELIEVE THESE FIELDS WERE POPULATED VIA A PUBLICLY AVAILABLE LIST OF US LOCATIONS, BASED ON THE LESS WELL-KNOWN CITY NAMES AND THE LACK OF SPACING FOR TWO-WORD NAMES (SUCH AS “FORTSENECA” FOR FORT SENECA, OHIO OR “CEDARMOUNTAIN” FOR CEDAR MOUNTAIN, VIRGINIA).

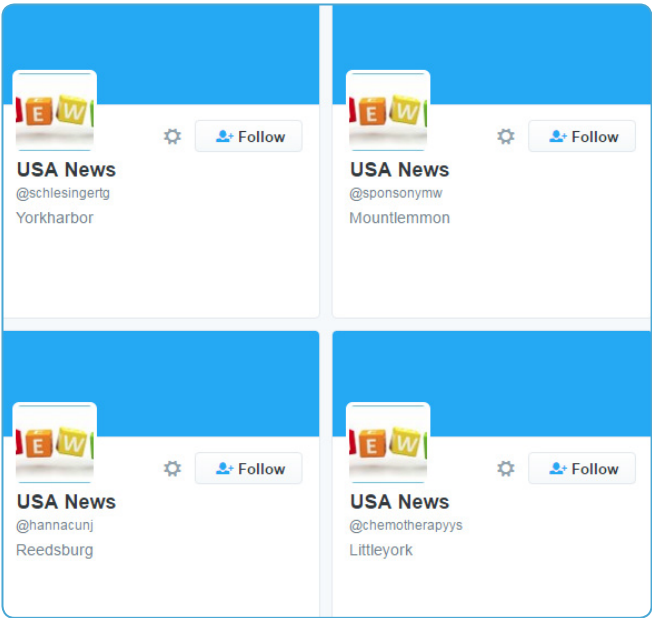


FIGURE 3.3.28: ACCOUNTS BELONGING TO THE “USA NEWS” WARLIST, WHICH PROMOTED THREAT ACTIVITY FOR @ANPOLAND. WE BELIEVE THESE FIELDS WERE POPULATED VIA THE SAME SOURCE USED FOR THE ACCOUNTS IN FIGURE 3.3.24 ABOVE, AND FOR THE SAME REASONS. NOTICE, FOR EXAMPLE, “MOUNTLEMMON” IS USED INSTEAD OF THE CORRECT FORM, MOUNT LEMMON.⁹

Accounts Tweet Identical or Very Similar Content

In all instances, Warlist accounts tweeted identical or very similar content in their promotion of cyber threat activity and political narratives.

USERNAME	DISPLAY NAME	TWEET	TIMESTAMP (EST)
@antibank_	AntiBank	@LouisPeitzman @jimwaterson Pls, its very important! Qatarbank was hacked. Link for Archive pin on my top. [link to download]	6:14
@antibank__	AntiBank	@karadolman Pls, its very important! Qatarbank was hacked. Link for Archive pin on my top. [link to download]	6:19
@antibank__	AntiBank	@DanielJonesSun Pls, its very important! Qatarbank was hacked. Link for Archive pin on my top. [link to download]	6:19
@antibank__	AntiBank	@LauraSunShowbiz Pls, its very important! Qatarbank was hacked. Link for Archive pin on my top. [link to download]	6:21
@antibank__	AntiBank	@JennyFrancis23 Pls, its very important! Qatarbank was hacked. Link for Archive pin on my top. [link to download]	6:22
@antibank__	AntiBank	@Nick_TheSun Pls, its very important! Qatarbank was hacked. Link for Archive pin on my top. [link to download]	6:23
@antibank_	AntiBank	@HayesBrown @shani_o @schoofsFeed Pls, its very important! Qatarbank was hacked. Link for Archive pin on my top. [link to download]	6:24
@antibank_	AntiBank	@SteveKandell @ifyouseekjaimie Pls, its very important! Qatarbank was hacked. Link for Archive pin on my top. [link to download]	6:25

FIGURE 3.3.29: IDENTICAL CONTENT (DIRECTED AT DIFFERENT RECIPIENTS) TWEETED BY SAMPLE ACCOUNTS FROM THE “ANTIBANK” WARLIST IN APRIL 2016, WHICH PROMOTED BOZKURT HACKERS’ THREAT ACTIVITY AGAINST QATAR NATIONAL BANK.

USERNAME	DISPLAY NAME	TWEET	TIMESTAMP (EST)
@uncinusp	China Daily	@cspan #hacked Large Laboratory in the USA [link to download]	6:54
@uncoversm	China Daily	@PressClubDC #hacked Large Laboratory in the USA [link to download]	6:54
@unemploymentpc	China Daily	@errolmorris #hacked Large Laboratory in the USA [link to download]	6:55
@unicuspidw	China Daily	@TimothyS #hacked Large Laboratory in the USA [link to download]	6:55
@untoldlq	China Daily	@amnesty #hacked Large Laboratory in the USA [link to download]	6:55
@uranusvb	China Daily	@USGAO #hacked Large Laboratory in the USA [link to download]	6:55
@vaishbe	China Daily	@cyberwar #hacked Large Laboratory in the USA [link to download]	6:55
@vandavandalq	China Daily	@NoahShachtman #hacked Large Laboratory in the USA [link to download]	6:55
@vernationt	China Daily	@pressfreedom #hacked Large Laboratory in the USA [link to download]	6:56
@villousv	China Daily	@DMLPBerkman #hacked Large Laboratory in the USA [link to download]	6:56

FIGURE 3.3.30: IDENTICAL CONTENT (DIRECTED AT DIFFERENT RECIPIENTS) TWEETED BY SAMPLE ACCOUNTS FROM THE “CHINA DAILY” WARLIST ON AUGUST 2, 2016, WHICH PROMOTED @PRAVSECTOR’S CLAIMED DATA LEAK FROM THE CENTRAL OHIO UROLOGY CLINIC.

USERNAME	DISPLAY NAME	TWEET	TIMESTAMP (EST)
@accumulationg	China Daily	@RSnake Leak International Court of Arbitration [link to download]	2:47:44
@barcroftew	China Daily	@nyxbone Leak International Court of Arbitration [link to download]	2:47:49
@bessevyk	China Daily	@SecurityBeard Leak International Court of Arbitration [link to download]	2:48:14
@blankabbb	China Daily	@Riana_Crypto Leak International Court of Arbitration [link to download]	2:48:28
@bouffantml	China Daily	@ezequielvazquez Leak International Court of Arbitration [link to download]	2:49:01
@boylangk	China Daily	@AndresDelgadoEC Leak International Court of Arbitration [link to download]	2:49:09
@calzadaey	China Daily	@DrWhax Leak International Court of Arbitration [link to download]	2:49:58
@clemmersn	China Daily	@Scott_Helme Leak International Court of Arbitration [link to download]	2:50:45
@coolidgeho	China Daily	@vinnie Leak International Court of Arbitration [link to download]	2:51:30
@copyli	China Daily	@NASAWatch Leak International Court of Arbitration [link to download]	2:51:36

FIGURE 3.3.31: IDENTICAL CONTENT (DIRECTED AT DIFFERENT RECIPIENTS) TWEETED BY SAMPLE ACCOUNTS FROM A DIFFERENT “CHINA DAILY” WARLIST ON AUGUST 10, 2016, WHICH PROMOTED @ANPOLAND’S CLAIMED DATA LEAK FROM THE COURT OF ARBITRATION FOR SPORT. THE “CHINA DAILY” WARLISTS WERE THE ONLY INSTANCE WE OBSERVED IN WHICH TWO DIFFERENT PERSONAS, @PRAVSECTOR AND @ANPOLAND, USED IDENTICAL LANGUAGE AND ICONOGRAPHY FOR DISTINCT WARLISTS.

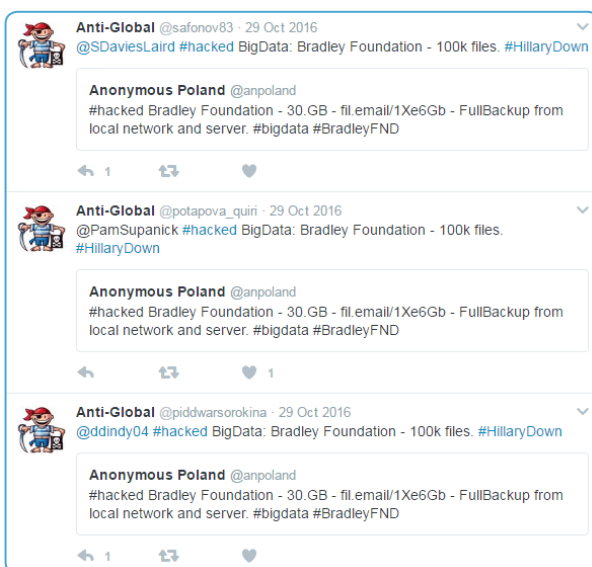


FIGURE 3.3.32: IDENTICAL CONTENT (DIRECTED AT DIFFERENT RECIPIENTS) TWEETED BY SAMPLE ACCOUNTS FROM THE “ANTI-GLOBAL” WARLIST IN OCTOBER 2016, WHICH PROMOTED @ANPOLAND’S CLAIMED DATA LEAK FROM THE BRADLEY FOUNDATION.

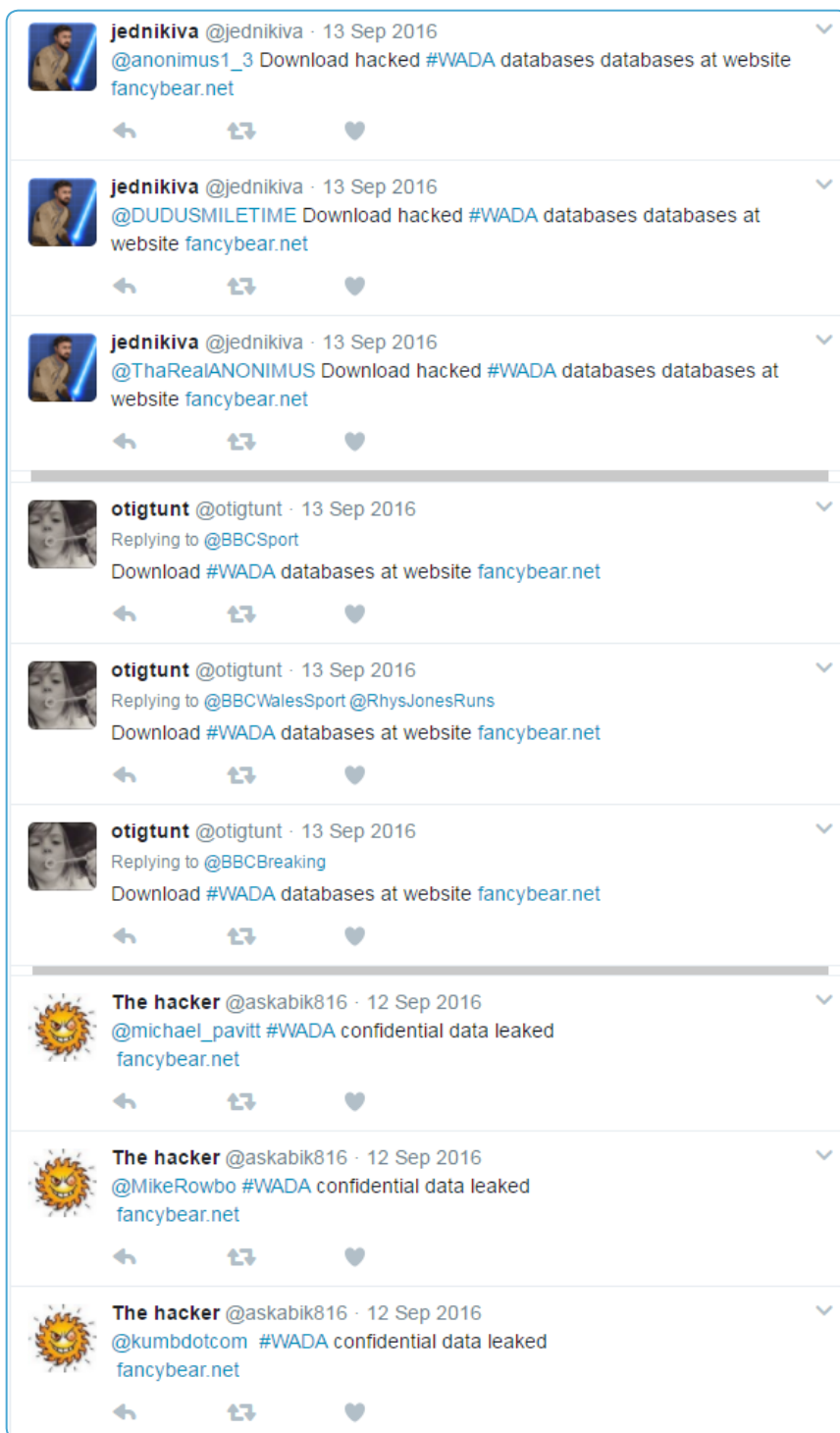


FIGURE 3.3.33: COLLECTION OF SCREENSHOTS ILLUSTRATING CONTENT FROM A WARLIST IN SEPTEMBER 2016 WHICH PROMOTED FANCY BEARS' HACK TEAM'S CLAIMED DATA LEAK FROM WADA. CONTENT IS IDENTICAL IN EACH TWEET BY AN INDIVIDUAL ACCOUNT AND SIMILAR ACROSS THE THREE ACCOUNTS. THIS WARLIST DID NOT FEATURE IDENTICAL PROFILE PICTURES OR DISPLAY NAMES.

The Adoption of False Personas

In several cases, Warlist accounts used display names and profile pictures that presented the users as journalists or political activists. We assess with high confidence that these attempts were designed to mask the accounts' true nature, and in the case of journalistic facades, was also likely intended to give the impression of significance and/or impartiality to promoted content.

USERNAME	DISPLAY NAME	TWEET	TIMESTAMP (EST)
@jazeera_19	Al Jazeera	@MIAuniverse Turkish hackers were behind the Qatar Bank data breach [link to download]	20:48
@jazeera_2	Al Jazeera	@energyintel Turkish hackers were behind the Qatar Bank data breach [link to download]	20:48
@jazeera_20	Al Jazeera	@deborahamos Turkish hackers were behind the Qatar Bank data breach [link to download]	20:48
@jazeera_5	Al Jazeera	@arezaian Turkish hackers were behind the Qatar Bank data breach [link to download]	20:48
@jazeera_6	Al Jazeera	@AliTahmizian Turkish hackers were behind the Qatar Bank data breach [link to download]	20:48
@qatar_air_1	Qatar Airways	@mhnaajmi64 Turkish hackers were behind the Qatar Bank data breach [link to download]	20:48
@qatar_air_10	Qatar Airways	@baeidinejad Turkish hackers were behind the Qatar Bank data breach [link to download]	20:48
@qatar_air_11	Qatar Airways	@golnarM Turkish hackers were behind the Qatar Bank data breach [link to download]	20:48
@qatar_air_12	Qatar Airways	@PostBardon Turkish hackers were behind the Qatar Bank data breach [link to download]	20:48

FIGURE 3.3.34: ACCOUNTS IN TWO WARLISTS RELATED TO BOZKURT HACKERS. THE FIRST SET FEATURED A PROFILE PICTURE (NOT SHOWN) AND DISPLAY NAME THAT INDICATED ASSOCIATION WITH THE LEGITIMATE QATAR-BASED NEWS OUTLET AL JAZEERA, WHILE THE SECOND SET FEATURED A PROFILE PICTURE (NOT SHOWN) AND DISPLAY NAME THAT INDICATED ASSOCIATION WITH THE LEGITIMATE AIRLINE QATAR AIRWAYS.

USERNAME	DISPLAY NAME	TWEET	TIMESTAMP (EST)
@mediocrityzn	EuroPress	@innesbowen #hacked Big Laboratory in USA [link to download]	9:52
@metastasizet	EuroPress	@Eilas1 #hacked Big Laboratory in USA [link to download]	9:52
@monegasquesl	EuroPress	@desk_poloracle #hacked Big Laboratory in USA [link to download]	9:52
@nankeenb	EuroPress	@LenaDeWinne #hacked Big Laboratory in USA [link to download]	9:52
@nasaado	EuroPress	@Room_Space #hacked Big Laboratory in USA [link to download]	9:52
@navarinofm	EuroPress	@Deeyah_Khan #hacked Big Laboratory in USA [link to download]	9:52
@newportsyf	EuroPress	@sally19853 #hacked Big Laboratory in USA [link to download]	9:52
@nonexistenceaa	EuroPress	@michealevans #hacked Big Laboratory in USA [link to download]	9:52

FIGURE 3.3.35: ACCOUNTS IN A WARLIST RELATED TO @PRAVSECTOR. THE EUROPEAN UNION-THEMED PROFILE PICTURE (NOT SHOWN) AND DISPLAY NAME, "EURO PRESS," IMPLIED THAT THE ACCOUNTS WERE RELATED TO A JOURNALISTIC ENTITY THAT REPORTS ON EUROPEAN UNION-RELATED NEWS.

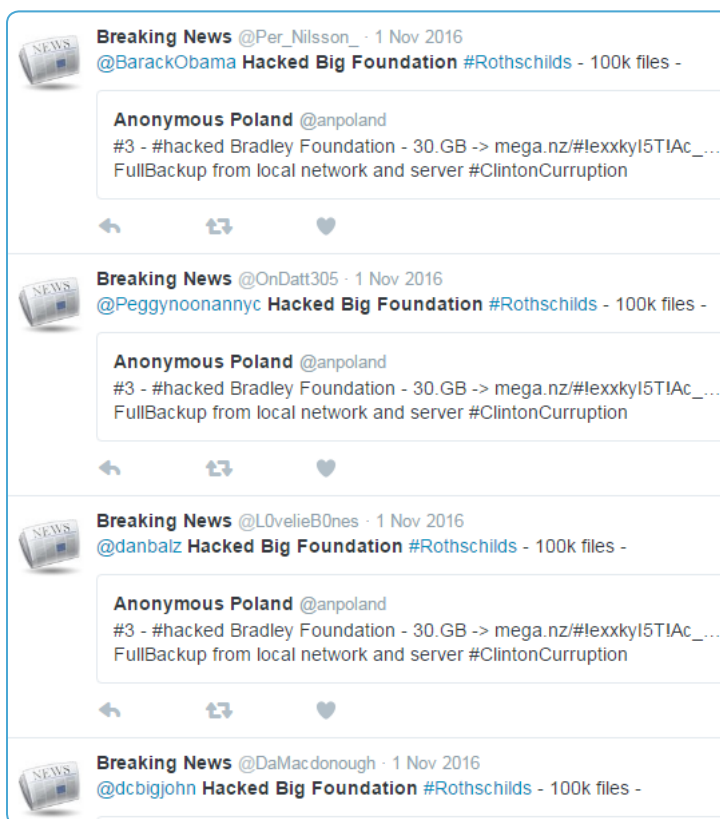


FIGURE 3.3.36: ACCOUNTS IN A WARLIST RELATED TO @ANPOLAND. THE GENERIC PROFILE PICTURE AND DISPLAY NAME SUGGESTED THAT THE ACCOUNTS WERE EITHER RELATED TO A LEGITIMATE JOURNALISTIC ENTITY OR WERE SIMPLY AUTOMATED ACCOUNTS THAT SHARED ENGLISH-LANGUAGE NEWS. NOTE THAT THE ACCOUNTS USED THE HASHTAG #ROTHSCHILDS IN THEIR MESSAGING, A COMMON THEME WE HAVE OFTEN OBSERVED USED BY "TROLL" SOCIAL MEDIA ACCOUNTS ATTEMPTING TO DISCREDIT THE "GLOBAL ELITE."



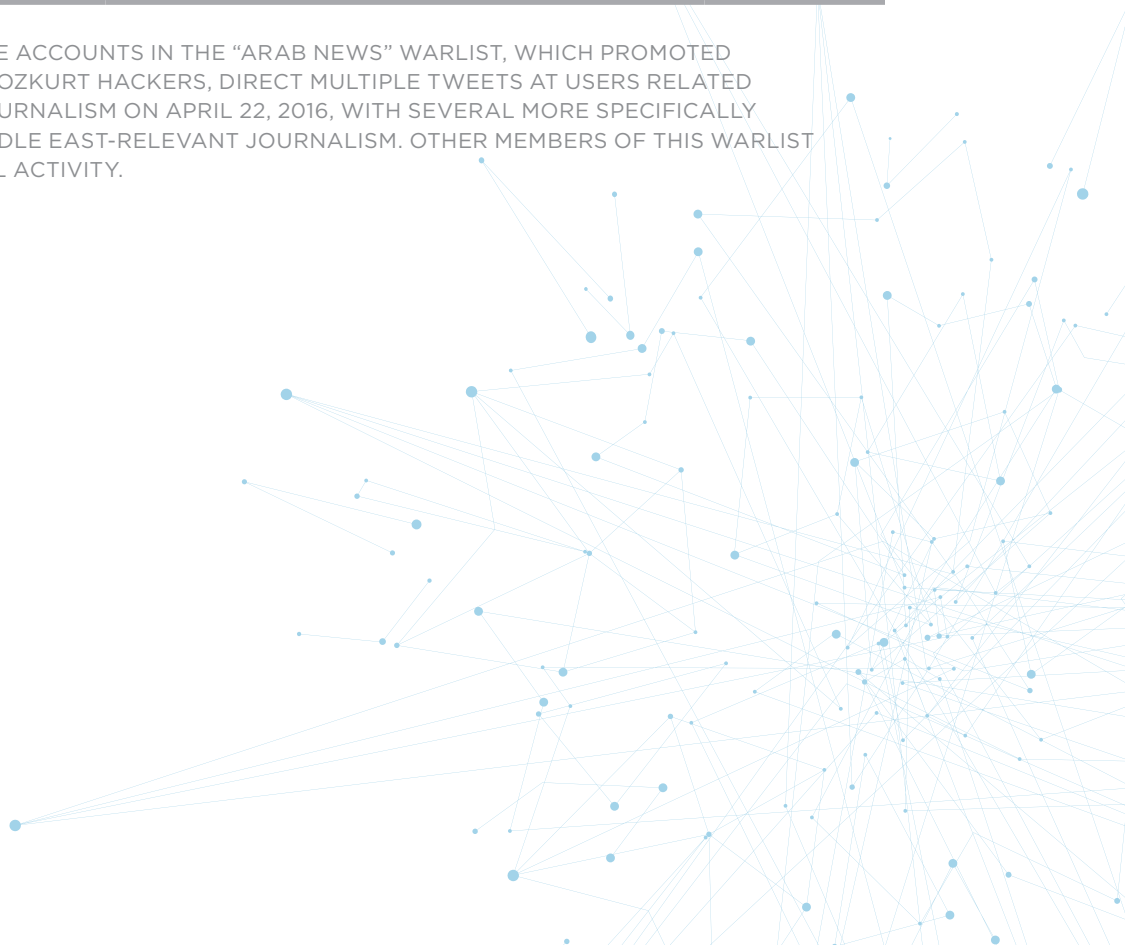
FIGURE 3.3.37: SAMPLE ACCOUNTS IN THE @ANPOLAND-ASSOCIATED #WARAGAINSTDEMOCRATS WARLIST. FEATURES APPEAR TO PORTRAY THE ACCOUNTS AS US-BASED USERS SUPPORTIVE OF THE REPUBLICAN PARTY. SEVERAL OF THESE ACCOUNTS POSTED NON-US-RELATED CONTENT IN LANGUAGES OTHER THAN ENGLISH IN YEARS PRIOR TO 2016; THAT AND OTHER ACTIVITY SUGGESTS THAT THEY WERE USED AS PART OF MULTIPLE PROMOTIONAL CAMPAIGNS BETWEEN 2013 AND 2016. THIS DIFFERENTIATES THESE ACCOUNTS FROM THOSE IN OTHER WARLISTS, WHICH APPEARED TO HAVE BEEN COMPILED SPECIFICALLY FOR THEIR RESPECTIVE CAMPAIGNS.

The Directing of Tweets at Other, Legitimate Twitter Users (Indirect Advocacy)

Warlists were almost exclusively used to engage in indirect advocacy, with accounts tweeting directly at individuals and organizations that might potentially amplify news of leak activity and associated political narratives. For example, we recorded several instances of Warlists directing tweets at hundreds or thousands of other Twitter users, with recipients appearing to have been organized into distinct lists based on location, field, or political affiliation.

USERNAME	DISPLAY NAME	TWEET	TIMESTAMP (EST)
@arab_news2	Arab News	@sham_jaff Qatarbank was hacked. Link for Archive pin on my top.	22:14
@_arab_news__	Arab News	@ErinCarson Qatarbank was hacked. Link for Archive pin on my top	22:15
@arab_news2	Arab News	@pauliddon Qatarbank was hacked. Link for Archive pin on my top	22:21
@_arab_news__	Arab News	@annieisi Qatarbank was hacked. Link for Archive pin on my top	22:21
@arab_news2	Arab News	@NWaisy Qatarbank was hacked. Link for Archive pin on my top	22:23
@_arab_news__	Arab News	@markdubya Qatarbank was hacked. Link for Archive pin on my top	22:23
@arabnews____0	Arab News	@npwcnn Qatarbank was hacked. Link for Archive pin on my top	22:44

FIGURE 3.3.38: : SAMPLE ACCOUNTS IN THE “ARAB NEWS” WARLIST, WHICH PROMOTED THREAT ACTIVITY BY BOZKURT HACKERS, DIRECT MULTIPLE TWEETS AT USERS RELATED TO INTERNATIONAL JOURNALISM ON APRIL 22, 2016, WITH SEVERAL MORE SPECIFICALLY ASSOCIATED WITH MIDDLE EAST-RELEVANT JOURNALISM. OTHER MEMBERS OF THIS WARLIST ENGAGED IN IDENTICAL ACTIVITY.



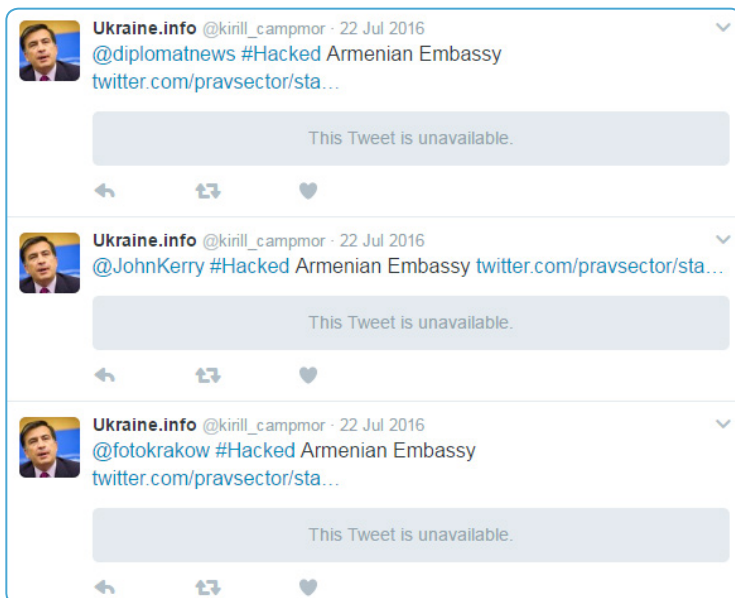


FIGURE 3.3.39: AN ACCOUNT IN THE "UKRAINE.INFO" WARLIST THAT PROMOTED THREAT ACTIVITY BY @PRAVSECTOR DIRECTS MULTIPLE TWEETS AT USERS BROADLY RELEVANT TO EUROPEAN DIPLOMACY OR POLITICS ON JULY 22, 2016. OTHER MEMBERS OF THIS WARLIST ENGAGED IN IDENTICAL ACTIVITY.

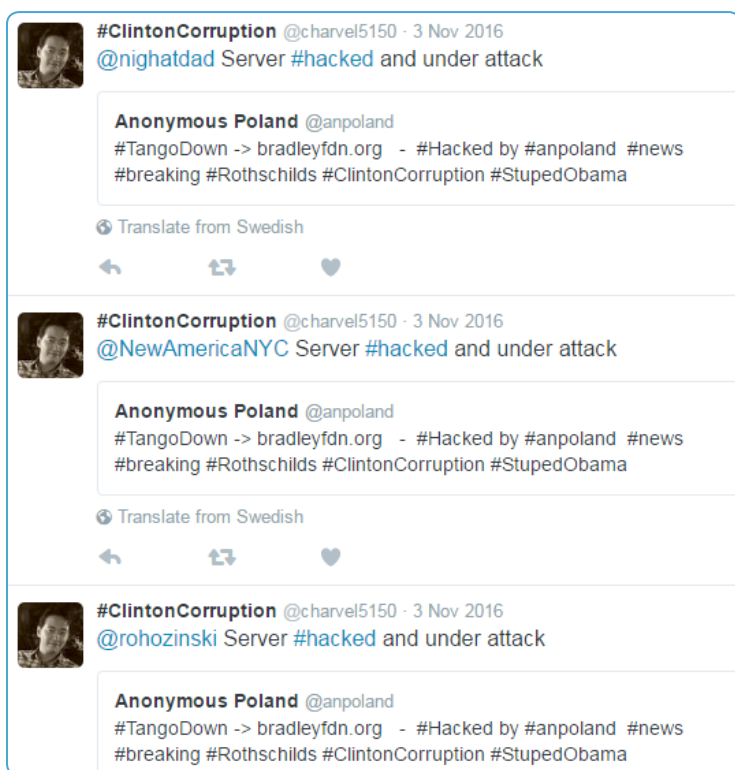


FIGURE 3.3.40: AN ACCOUNT IN THE #CLINTONCORRUPTION WARLIST THAT PROMOTED THREAT ACTIVITY BY @ANPOLAND DIRECTS MULTIPLE TWEETS AT USERS BROADLY RELEVANT TO INFORMATION SECURITY ON NOV. 3, 2016. OTHER MEMBERS OF THIS WARLIST ENGAGED IN IDENTICAL ACTIVITY.

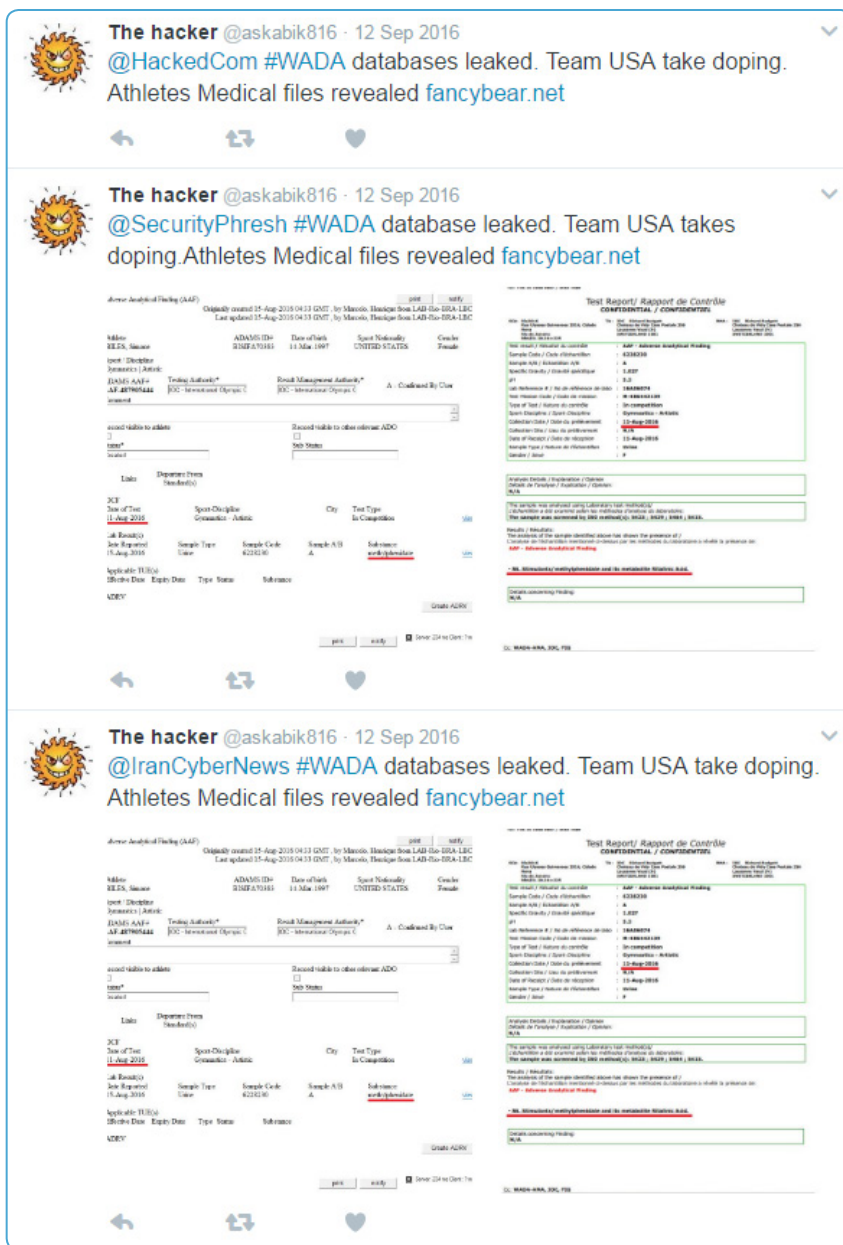


FIGURE 3.3.41: AN ACCOUNT IN A WARLIST THAT PROMOTED THREAT ACTIVITY BY FANCY BEARS' HACK TEAM TWEETS MULTIPLE MESSAGES AT TWITTER USERS IN THE FIELD OF INFORMATION SECURITY ON SEP. 12, 2016. OTHER MEMBERS OF THIS WARLIST ENGAGED IN SIMILAR ACTIVITY.

Appendix: Timeline of Activity

DATE	ACTOR	ACTIVITY
4/23/2010	@anpoland	@anpoland Twitter account created. Aside from one Tweet in April 2010 and two retweets in January and February 2012, the account appears to have been dormant until it threatened leak activity in a tweet directed at @pravsector on July 29, 2016.
11/9/2015		The World Anti-Doping Agency (WADA) Independent Commission, chaired by Richard Pound, releases findings of misconduct by Russian anti-doping authorities ⁸⁵
11/10/2015		WADA suspends accreditation of the Moscow Antidoping Center laboratory following the release of the Independent Commission report ⁸⁶
11/17/2015	Bozkurt Hackers	Hacker Buba begins publishing tweets containing alleged account data belonging to InvestBank customers
11/18/2015		WADA declares six National Anti-Doping Organizations (NADOs), including the Russian Anti-Doping Organization (RUSADA), non-compliant ⁸⁷
11/21/2015	CyberBerkut	CyberBerkut claims to leak documents demonstrating that Ukrainian company UkrOboronProm sold weapons to Qatar through Polish military contractor Level 11, and implies that Qatar then supplied those weapons to extremists in Syria.
12/3/2015	Bozkurt Hackers	Hacker Buba posts a download link to approximately 250MB of alleged InvestBank account data to Twitter, claiming to have previously attempted to extort InvestBank
12/7/2015	CyberBerkut	CyberBerkut claims to leak additional documents allegedly demonstrating that the Ukrainian defense industrial base company SpetsTechnoExport, a subsidiary of UkrOboronProm, sold weapons to Qatar through Polish company Level 11. CyberBerkut claims that the weapons purchased are not compatible with Qatar's French-made military aircraft, and again argues that Qatar could be supplying the weapons to extremists in Syria.
1/3/2016	CyberBerkut	CyberBerkut claims to have accessed Android phones belonging to Ukrainian fighters in the "Azov" battalion, and posts a video and photos allegedly providing evidence that ISIS militants are fighting with Ukrainians against the Donetsk separatists. The video, photos, and claims of alleged ISIS involvement were later debunked by the BBC. ⁸⁸

⁸⁵ <https://www.wada-ama.org/en/resources/world-anti-doping-program/independent-commission-report-1>

⁸⁶ <https://www.wada-ama.org/en/media/news/2015-11/wada-acts-immediately-to-suspend-accreditation-of-moscow-laboratory>

⁸⁷ <https://www.wada-ama.org/en/media/news/2015-11/foundation-board-media-release-wada-strengthens-anti-doping-worldwide>

⁸⁸ http://www.bbc.com/russian/features-38109630?ocid=socialflow_twitter

February 2015 – July 2016	APT28	APT28 targets Bellingcat contributors in several waves of phishing using shortened bit.ly links ⁸⁹
2/10/2016	CyberBerkut	CyberBerkut defaces the Bellingcat website. ⁹⁰ Bellingcat is an investigative research and investigative journalism group that contributed to the MH-17 investigation.
2/19/2016	CyberBerkut	CyberBerkut claims to leak a document drafted by the head of the Foreign Intelligence Service of Ukraine containing plans to coerce Dutch officials ahead of the April 6, 2016 referendum in the Netherlands to approve or disapprove of the Association Agreement between the European Union and Ukraine.
2/24/2016	CyberBerkut	CyberBerkut leaks PII and personal photos of Ruslan Leviev, a blogger and Bellingcat researcher who has written articles critical of the Kremlin
March - April 2016	APT28	APT28 phishing campaign targets the DCCC ⁹¹
3/1/2016		"Super Tuesday" in US Democratic and Republican Presidential primary races
mid-March to mid-May 2016	APT28	APT28 phishing campaign using bit.ly shortened links targets Hillary for America (hillaryclinton.com) email accounts, according to Dell Secure Works ⁹²
mid-March to mid-April 2016	APT28	APT28 phishing campaign using bit.ly shortened links targets DNC (dnc.org) email accounts, according to Dell Secure Works ⁹³
3/19/2016	APT28	Clinton presidential campaign Chairman John Podesta receives fake Google password reset email with shortened bit.ly link leading to a malicious credential collection page FireEye iSIGHT Intelligence attributed to APT28
3/22/2016	APT28	Clinton campaign staffer William Rinehart receives phishing email that leads to a malicious credential collection page FireEye iSIGHT Intelligence attributed to APT28 ⁹⁴
3/22/2016	APT28	The domain misdepartrment.com, possibly spoofing DNC IT services provider, is registered ⁹⁵
3/26/2016	Bozkurt Hackers	A "guest" user posts a link to a Google Drive hosting additional alleged InvestBank account holder data to Pastebin ⁹⁶
3/28/2016	Bozkurt Hackers	The user "bozkurt.3754" posts a link to the same Google Drive hosting additional alleged InvestBank account holder data to a cybercrime forum
April 2016	APT28	APT28 gains access to DNC systems, according to CrowdStrike ⁹⁷
4/1/2016	CyberBerkut	CyberBerkut leaks documents allegedly belonging to a Ukrainian parliamentary delegation that visited Belgium and the Netherlands.

⁸⁹ <https://www.threatconnect.com/blog/russia-hacks-bellingcat-mh17-investigation/>

⁹⁰ <https://twitter.com/bellingcat/status/697334674029412353>

⁹¹ <http://www.nytimes.com/2016/12/13/us/politics/house-democrats-hacking-dccc.html>

⁹² <https://www.secureworks.com/research/threat-group-4127-targets-hillary-clinton-presidential-campaign>

⁹³ <https://www.secureworks.com/research/threat-group-4127-targets-hillary-clinton-presidential-campaign>

⁹⁴ <http://www.thesmokinggun.com/documents/investigation/tracking-russian-hackers-638295>

⁹⁵ <https://www.threatconnect.com/blog/tapping-into-democratic-national-committee/>

⁹⁶ <https://pastebin.com/p8pEiUct>

⁹⁷ <https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/>

4/4/2016	CyberBerkut	CyberBerkut claims to have maintained access to the network of the Ukrainian President's Administration and leaks an alleged decree to "gift" a Ukrainian oblast to Turkey and Crimean Tatars for settlement. This document is likely fake.
4/12/2016	DC Leaks	electionleaks.com website registered
4/16/2016	@pravsektor	"Ukraine.info" Warlist created
4/17-18/2016	Bozkurt Hackers	"QNB" Warlist created
4/17-26/2016	@anpoland	"Anti-Global" Warlist created
4/19/2016	DC Leaks	DC Leaks.com website registered
4/20/2016	Bozkurt Hackers	Bozkurt Hackers leaks alleged account and transaction data from Qatar National Bank (QNB) using several Twitter accounts using variations on the name "Anti QNB," for example @q_n_b1
4/21/2016	Bozkurt Hackers	"Anti-QNB" Warlist promotes Bozkurt Hackers activity
4/22-23/2016	Bozkurt Hackers	"QNB," "Arab News," and "Anti-Bank" Warlists promote Bozkurt Hackers activity
4/24-25/2016	Bozkurt Hackers	"AntiQatar" Warlist promotes Bozkurt Hackers activity
5/1-2/2016	Bozkurt Hackers	"Qatar Airways" and "Al Jazeera" Warlists promote Bozkurt Hackers activity
5/6/2016	Bozkurt Hackers	Bozkurt Hackers leaks additional alleged InvestBank account data
5/9/2016	Bozkurt Hackers	Bozkurt Hackers claims to leak data from Nepalese banks Business Universal Development Bank (data apparently stolen from an email server), and Sanima Bank (account and transaction information); Bangladeshi banks Dutch-Bangla Bank (ATM transaction information, employee logins), The City Bank (customer PII), Trust Bank (employee login credentials); and Sri Lankan bank the Commercial Bank of Ceylon (employee logins)
June 1 or 2, 2016	@pravsektor	@pravysektor Twitter account registered
6/4/2016	DC Leaks	DC Leaks publishes correspondence allegedly belonging to military contractors, CENTCOM personnel, Republican Party employees, and campaign staffers for Senators John McCain, Lindsey Graham, and other individuals
6/7/2016	DC Leaks	DC Leaks releases documents including Clinton tax returns, memos, staffer biographies, and reports from the William J. Clinton Presidential Library; a Library spokesperson confirmed that the documents were publicly available via the Library's website ⁹⁸
6/8/2016	DC Leaks	Twitter account @DCLeaks_ is created
6/8/2016	DC Leaks	DC Leaks claims to leak summaries of media reporting compiled by Hillary Clinton campaign staffers, and email correspondence belonging to Former NATO Commander and retired US General Philip Breedlove (postdated 4/10/16)
6/14/2016	APT28	APT28 registers actblues.com; FireEye iSIGHT Intelligence believes this spoofed domain was used to compromise the "donate" function of the DCCC website for an unknown duration that included the period June 19-27, 2016. The site may have also been compromised for periods before and after those dates.

⁹⁸ <https://www.stripes.com/news/russian-hackers-of-dnc-said-to-scoop-up-secrets-from-nato-soros-1.423578>

6/14/2016		CrowdStrike publishes a blog post attributing two separate compromises of the DNC to APT28 and APT29 ⁹⁹
6/15/2016	Guccifer 2.0	Guccifer 2.0 leaks data allegedly stolen from the DNC via a dedicated blog and direct leaks to media outlets The Hill, The Smoking Gun, and Gawker
6/18/2016	Guccifer 2.0	Guccifer 2.0 leaks additional alleged DNC documents, including financial reports and donors' PII
6/20/2016	Guccifer 2.0	@Guccifer_2 Twitter account created, links to the Guccifer 2.0 WordPress site
6/21/2016	Guccifer 2.0	Guccifer 2.0 leaks alleged DNC files on Hillary Clinton including memos, defensive strategies regarding issues including Clinton's classified email scandal, expense lists, and donor lists
6/21/2016	Guccifer 2.0	Motherboard publishes interview with Guccifer 2.0 in which Motherboard attempts to communicate with the persona in Romanian, but subsequent Motherboard linguistic analysis suggests that Guccifer 2.0 is not a native speaker of Romanian ¹⁶
6/22/2016	Guccifer 2.0	Guccifer 2.0 announces upcoming FAQ, calls for journalists, others to submit questions through Twitter
6/30/2016	Guccifer 2.0	Guccifer 2.0 publishes FAQ on WordPress page
7/4/2016	Guccifer 2.0	Guccifer 2.0 retweets WikiLeaks' claimed leak of Hillary Clinton emails on Iraq
7/1-7/2016	@pravsector	@pravsector Twitter account is registered
7/6/2016	Guccifer 2.0	Guccifer 2.0 leaks additional alleged DNC documents including the DNC action plan for the Republican National Convention, a May 16, 2016 "Event Memo" detailing logistics for President Obama's appearance at a May 18 DNC fundraising event in Washington D.C., a DNC LGBT event guest list, and donor information
7/7/2016	@pravsector	@pravsector claims to leak approximately 14 GB of data from Polish telecommunications company Netia. Leaked data includes customers' personally identifiable information (PII) and employee login credentials. @pravsector statements include disparaging references to the Polish Senate's vote to recognize the Volhynia and Galicia massacres as genocide, and other offensive and racially charged language.
7/7/2016	@pravsector	"Poland News" and "Lemberg" Warlists promote Netia data leak
7/8/2016	@anpoland	"USA News" Warlist created
7/8/2016		North Atlantic Treaty Organization (NATO) summit in Warsaw
7/13/2016	DC Leaks	DC Leaks publishes emails purportedly stolen from Clinton campaign staffer Sarah Hamilton
7/13/2016	Guccifer 2.0	Guccifer 2.0 leaks roughly 700 MB of alleged DNC data during the persona's "talk" at a London cybersecurity conference (the talk was delivered by a third party and read aloud from a script); data includes PII of top Obama White House officials, and Virginia Senator/Democratic Vice Presidential Candidate Tim Kaine's personal cell phone number

⁹⁹ https://motherboard.vice.com/en_us/article/dnc-hacker-guccifer-20-full-interview-transcript; https://motherboard.vice.com/en_us/article/why-does-dnc-hacker-guccifer-20-talk-like-this

7/14/2016	Guccifer 2.0	Guccifer 2.0 leaks additional purported DNC documents, including data on contributions from Norman Hsu (the convicted pyramid investment promoter who was previously a fundraiser for the Democratic party), opposition research on Sarah Palin, and additional donor information
7/14-15/2016	@pravsector	@pravsector claims to leak data from the Polish Ministry of Defense (MOD) and makes statements referencing the US PRISM surveillance program that imply a connection between the MOD and US surveillance activities. @pravsector also threatens to release additional information from the MOD if the Polish Government does not pay a ransom of \$50,000 US. We doubt that the extortion attempt was intended to generate profit for the group; rather we believe that the extortion claim, and the use of a famous Right Sector member's bitcoin wallet, were intended to call additional attention to the leak.
7/18/2016		WADA publishes McLaren independent investigation report about Russian state manipulation of athlete doping control process; WADA recommends banning Russian athletes from the 2016 Olympics and Paralympics ¹⁰⁰
7/18-21/2016		Republican National Convention
7/18/2016	@pravsector	@pravsector claims to leak data from German investment firm Gap Vermögensverwaltung GmbH along with the words "Hello, Frau Merkel !" The data primarily consists of Excel spreadsheets, Word documents, and email messages (MSG), as well as JPEG and PDF files. GAP customer PII, PII of GAP employees, and plaintext employee usernames and passwords are also included in the leak.
7/18/2016	Guccifer 2.0	Guccifer 2.0 leaks second set of data exclusively to The Hill, including files allegedly regarding "political strategies, the upcoming Democratic National Convention and fundraising" ¹⁰¹
7/21/2016	@pravsector	@pravsector claims to leak login credentials for the Ukrainian Ministry of Foreign Affairs website, emails belonging to Ukrainian Minister of Internal Affairs Arsen Avakov, and data from the Armenian Embassy in Ukraine, accompanied with the words "@Fuck #Armenia #Fuck #Avakov." Minister Avakov is of Armenian descent.
7/21-8/1/2016	@pravsector	"Ukraine.info" Warlist promotes Armenian Embassy data leak
7/22/2016	WikiLeaks, Guccifer 2.0	WikiLeaks posts 20,000 alleged DNC emails. On the same day, Guccifer 2.0 claims to have provided the documents to WikiLeaks ¹⁰²
7/25-28/2016		Democratic National Convention
7/25/2016	@pravsector	@pravsector leaks additional data allegedly stolen from the Armenian Embassy in Ukraine
7/29/2016	@anpoland	@anpoland directs a tweet at @pravsector, a false hacktivist persona claiming Ukrainian affiliation. In the tweet, @anpoland threatens to conduct unspecified cyber threat activity in reaction to previous @pravsector activity targeting Polish government and commercial entities.

¹⁰⁰ <https://www.wada-ama.org/en/media/news/2016-07/wada-statement-independent-investigation-confirms-russian-state-manipulation-of>

¹⁰¹ <http://thehill.com/policy/cybersecurity/288119-new-guccifer-20-dump-highlights-wobbly-dems-on-iran-deal>

¹⁰² https://twitter.com/GUCCIFER_2/status/756530278982684672

7/29/2016		DCCC confirms that it has been the target of a "cybersecurity incident" that appears similar to activity targeting the DNC. Unnamed sources claim that the DCCC intrusion has been traced back to APT28 ¹⁰³
8/1/2016	@pravsector	@pravsector claims to leak data from the Central Ohio Urology Group, claiming that it demonstrates the "Pentagon conducted bacteriological [sic] tests in Ukraine." @pravsector also posts links to an InfoWars article alleging that the US military is testing biological weapons at laboratories in Ukraine, and a screenshot that appears to demonstrate the persona's unauthorized access to the Ohio Urology Clinic. @pravsector labeled the screenshot "hacked mil pc," perhaps to suggest that the clinic was somehow connected to the military.
8/1/2016	@anpoland	@anpoland claims to leak five sets of data allegedly belonging to the Ukrainian Government and NATO. The documents appear to be relatively mundane, including memos that appear to come from the Ukrainian Ministry of Foreign Affairs discussing cooperation with NATO, and sets of statistics that appear to come from the Ukrainian Ministry of Internal Affairs.
8/1/2016	CyberBerkut	CyberBerkut claims to leak documents from the Turkish Ministry of Defense and Foreign Intelligence service allegedly demonstrating that the Turkish Government provides financial support to Tatar militants in Crimea. The authenticity of these documents is unconfirmed.
8/1-2/2016	@pravsector	"IT News" and "News" Warlists promote @pravsector messaging
8/2/2016	@pravsector	@pravsector tweets a link to a Polish blog article comparing the Netia and Polish MoD breaches to the DNC breach, accompanied by the words "Yes, DNC + stuped [sic] Clinton = Trump" ¹⁰⁴
8/2/2016	@pravsector	"China Daily" and "EuroPress" Warlists promote @pravsector messaging
8/3/2016	@anpoland	@anpoland claims defacement of Ukrainian Government website for veterans
8/3/2016	APT28	wada-awa.org registered; we assess it to be controlled by APT28
8/4-13/2016 (approximate dates)	APT28	APT28 sends phishing emails to users of WADA's ADAMS database ¹⁰⁵
8/5-8/25/2016		2016 Olympic Games
8/8/2016	APT28	tas-cass.org, wada-arna.org registered; we assess that these domains are also controlled by APT28
8/10/2016	@anpoland	@anpoland claims to leak data from the Court of Arbitration for Sport (CAS), the Detroit Police Department, and data allegedly related to the Boeing KC-10 aircraft and the US Air Force Strategic Air Command. In a video, @anpoland displays the websites of CAS and WADA, both of which appear to have been defaced with news article headlines stating, "WE FORGOT THE SPORT IS OUT OF THE POLITIC. PLEASE FORGIVE US [sic];" we were unable to independently corroborate these claimed defacements.
8/10-11/2016	@anpoland	"USA News," "China Daily," and "News" Warlists promote @anpoland's claimed leak of data from US Strategic Air Command, Boeing, and CAS, as well as @anpoland's claimed DDoS attack against CAS

¹⁰³ https://www.washingtonpost.com/world/national-security/fbi-probes-suspected-breach-of-dccc-computers-by-russian-hackers/2016/07/28/71210464-5536-11e6-b7de-dfe509430c39_story.html?utm_term=.02d91f5409fe

¹⁰⁴ <https://lawsec.net/2016/08/01/pravy-sector-and-dnc-leak-as-symptoms-of-new-trend-in-russian-cyber-operations/>

¹⁰⁵ <https://www.wada-ama.org/en/media/news/2016-08/wada-confirms-illegal-activity-on-yuliya-stepanovas-adams-account>

8/11/2016	@anpoland	@anpoland claims to have conducted a DDoS attack against the CAS website. We observed that the CAS website was unavailable immediately following the claim, indicating that the website had indeed been disabled. @anpoland also threatens to conduct a DDoS attack against, and to leak data from, the World Anti-Doping Agency (WADA).
8/12/2016	Guccifer 2.0	Guccifer 2.0 claims to leak data from the DCCC; some content subsequently removed from the persona's WordPress blog, including database of contact information for Democratic Members of Congress and lists of passwords seemingly for subscription resources and social media accounts used by DCCC staff ¹⁰⁶
8/13/2016		WADA confirms that the Anti-Doping Administration and Management System (ADAMS) user account belonging to Yuliya Stepanova, the Russian track and field athlete and whistleblower who called attention to Russian athlete doping, was compromised. WADA also confirms that phishing emails originated from the illegitimate domains wada-awa.org and wada-arna.org that spoofed the WADA website. ¹⁰⁷
8/15/2016	Guccifer 2.0	Guccifer 2.0 leaks alleged DCCC data regarding primaries in Florida, including briefings, memos, and files on primarily Democratic candidates. Documents on at least one Republican candidate, John Mica, are also present
8/18/2016		FBI publishes Flash report describing malicious activity targeting state election boards; ¹⁰⁸ the January 2017 Intelligence Community Assessment affirms that Russian government actors are responsible for state election board compromises ¹⁰⁹
8/21/2016	Guccifer 2.0	Guccifer 2.0 leaks alleged DCCC data regarding primaries in Pennsylvania, including memos and press statements about the candidates, and background research on the candidates and Pennsylvania's political climate
8/23/2016	Guccifer 2.0	Guccifer 2.0 leaks purported DCCC data exclusively to The Hill; documents include DCCC research, strategies, and polling information on Pennsylvania's contested primary for House seats ¹¹⁰
8/25 - 9/12/2016	APT28	APT28 uses compromised credentials of an International Olympic Committee (IOC) account created specifically for the 2016 Olympic Games, to access the WADA ADAMS database and steal data that is later published by Fancy Bears' Hack Team ¹¹¹
8/26/2016	DC Leaks	DC Leaks posts emails allegedly taken from US Navy Captain Carl Pistole
8/31/2016	Guccifer 2.0	Guccifer 2.0 claims to leak documents taken from Nancy Pelosi's computer, including documents regarding congressional races in Florida and Pennsylvania (part of the larger batch given exclusively to The Hill); Pelosi denies that the documents came from her PC ¹¹²

¹⁰⁶ <http://thehill.com/policy/cybersecurity/291375-wordpress-blocks-latest-guccifer-20-docs>

¹⁰⁷ <https://www.wada-ama.org/en/media/news/2016-08/wada-confirms-illegal-activity-on-yuliya-stepanovas-adams-account>

¹⁰⁸ https://s.yimg.com/dh/ap/politics/images/boe_flash_aug_2016_final.pdf

¹⁰⁹ https://www.dni.gov/files/documents/ICA_2017_01.pdf

¹¹⁰ <http://thehill.com/policy/cybersecurity/292391-exclusive-guccifer-20-hacked-memos-expand-on-pennsylvania-house-races>

¹¹¹ <https://www.wada-ama.org/en/media/news/2016-10/cyber-security-update-wadas-incident-response>

¹¹² <http://www.ibtimes.co.uk/nancy-pelosi-denies-pc-was-hacked-by-guccifer-2-0-still-blames-russia-1579738>

9/1/2016	Fancy Bears' Hack Team	The domains fancybear.net and fancybear.org are registered
9/1/2016	CyberBerkut	CyberBerkut claims to have leaked documents from the Ukrainian Government allegedly demonstrating a Ukrainian effort to destroy evidence that the Security Service of Ukraine (SBU) had engaged in torture of detainees ahead of a visit by the United Nations Subcommittee on Prevention of Torture. The authenticity of the documents is unconfirmed.
9/5/2016	@anpoland	@anpoland again threatens to release data stolen from WADA
9/6/2016	Fancy Bears' Hack Team	@FancyBears Twitter account created
9/6/2016	Guccifer 2.0	Guccifer leaks alleged internal DCCC memo to the Observer; Observer publishes an op-ed arguing that the memo reveals that the DCCC was cooperating with the Clinton campaign in 2015, prior to becoming the Democratic nominee, and noted this to be a violation of the DCCC charter, which mandates impartiality towards all Democratic candidates ¹¹³
9/7-18/2016		2016 Paralympic Games
9/7/2016	@anpoland	@anpoland releases two videos that depict claimed defacements of the official websites of the International Paralympic Committee (IPC; paralympic.org) and the US Olympic Committee (USOC; teamusa.org). There is some very limited evidence, namely third-party observation on social media, that @anpoland successfully defaced both websites, though it is also plausible that the defacements were falsified.
9/7/2016	@anpoland	@pahomovfiluc84, a Twitter account we later tied to the @anpoland-related "Anti-Global" Warlist, promotes @anpoland's announcement of the paralympic.org defacement
9/12/2016	Fancy Bears' Hack Team	@FancyBearsHT Twitter account created
9/12/2016	Fancy Bears' Hack Team	Fancy Bears' Hack Team leaks alleged confidential TUEs belonging to prominent US athletes from WADA
9/12-13/2016	Fancy Bears' Hack Team	Possible "The hacker" Warlist promotes WADA leak by Fancy Bears' Hack Team
9/13/2016		WADA confirms that an APT28 compromise of the ADAMS database led to the public release of athlete medical records ¹¹⁴
9/13/2016	Guccifer 2.0	Guccifer 2.0 leaks roughly 700 MB of alleged DNC data DNC during his talk at a London cybersecurity conference (talk was delivered by someone else, read aloud from script provided by Guccifer 2.0); data includes PII of top Obama White House officials, Tim Kaine's personal cell phone number
9/14/2016	DC Leaks	DC Leaks publishes emails allegedly belonging to former Secretary of State Gen. Colin Powell, including messages mentioning his views on presidential candidates Hillary Clinton and Donald Trump
9/14/2016	Fancy Bears' Hack Team	Fancy Bears' Hack Team leaks second set of athlete TUEs from WADA
9/14/2016		WADA confirms that confidential medical records of 25 athletes from eight countries were disclosed publicly following a compromise by APT28 ¹¹⁵

¹¹³ <http://observer.com/2016/09/new-guccifer-2-0-dccc-coordinated-with-clinton-campaign-in-2015/>

¹¹⁴ <https://www.wada-ama.org/en/media/news/2016-09/wada-confirms-attack-by-russian-cyber-espionage-group>

¹¹⁵ <https://www.wada-ama.org/en/media/news/2016-09/wada-confirms-another-batch-of-athlete-data-leaked-by-russian-cyber-hackers-fancy>

9/15/2016	Guccifer 2.0	Guccifer 2.0 leaks alleged DCCC research on districts and candidates, fundraising plans, and memos related to primaries in New Hampshire, Ohio, Illinois, and North Carolina
9/16/2016	Fancy Bears' Hack Team	Fancy Bears' Hack Team leaks third set of TUEs from WADA
9/16/2016		WADA confirms the disclosure of confidential medical data of 11 athletes from five countries following an APT28 compromise ¹¹⁶
9/19/2016	Fancy Bears' Hack Team	Fancy Bears' Hack Team leaks fourth set of TUEs from WADA
9/19/2016		WADA confirms the public disclosure of confidential athlete data, including data relating to 26 athletes from 10 countries. WADA asserts that the documents were compromised via an APT28 phishing campaign. ¹¹⁷
9/22/2016	DC Leaks	DC Leaks publishes emails allegedly taken from former White House and Clinton campaign staffer Ian Mellul
9/23/2016	Guccifer 2.0	Guccifer 2.0 leaks purported DCCC dossier on DCCC Chairman and New Mexico Congressman Rep. Ben Ray Lujan
9/23/2016	Fancy Bears' Hack Team	Fancy Bears' Hack Team leaks fifth set of TUEs from WADA
9/23/2016		WADA confirms that Fancy Bears' Hack Team released confidential medical data associated with 41 athletes from 13 countries. ¹¹⁸
9/26/2016		1st US Presidential debate
9/30/2016	DC Leaks	DC Leaks posts password protected folders for documents allegedly stolen from State Department employee Sarah Stoll and Clinton campaign staffer Beanca Nicholson on Twitter and then gives Politico the password ¹¹⁹
9/30/2016	Fancy Bears' Hack Team	Fancy Bears' Hack Team leaks sixth set of TUEs from WADA
10/3/2016		WADA confirms Fancy Bears' Hack Team released additional confidential athlete data "concerning 20 athletes from 14 countries" ¹²⁰
10/4/2016		US Vice Presidential debate
10/4/2016	WikiLeaks	WikiLeaks states that it will be releasing documents regarding the US elections and Google over the following ten weeks
10/4/2016	Guccifer 2.0	Guccifer 2.0 leaks alleged documents from the Clinton Foundation; documents appear to have actually come from the DCCC
10/4/2016	CyberBerkut	CyberBerkut claims to have leaked documents from the Ukrainian Government allegedly demonstrating that Ukrainian security agencies were obstructing Organization for Security and Cooperation in Europe (OSCE) monitoring efforts in Ukraine, that the Ukrainian State Border Guard Service was involved in smuggling petroleum products in to Europe, and that the Ukrainian Government was also involved in "legalizing" ISIS militants and allowing them to travel into Europe. The authenticity of these documents is unconfirmed.

¹¹⁶ <https://www.wada-ama.org/en/media/news/2016-09/wada-statement-regarding-additional-data-leak-via-russian-cyber-hacker-fancy-bear>

¹¹⁷ <https://www.wada-ama.org/en/media/news/2016-09/cyber-hack-update-data-leak-concerning-26-athletes-from-10-countries-and-12>

¹¹⁸ <https://www.wada-ama.org/en/media/news/2016-09/cyber-hack-update-data-leak-concerning-41-athletes-from-13-countries-and-17>

¹¹⁹ <http://www.politico.com/story/2016/09/russia-hackers-clinton-campaign-state-department-228976>

¹²⁰ <https://www.wada-ama.org/en/media/news/2016-10/cyber-hack-update-data-leak-concerning-20-athletes-from-14-countries-and-13>

10/5/2016		WADA releases a statement on the Fancy Bears' Hack Team data leaks, noting that not all data released by the persona accurately reflects ADAMS data. WADA also states that APT28 "illegally obtained the data from an [ADAMS] account" ¹²¹
10/6/2016	DC Leaks	DC Leaks publishes emails purportedly stolen from former US Chief of Protocol Capricia Marshall, whom DC Leaks describes as a Clinton loyalist and Washington insider. DC Leaks also states that Marshall was named in allegations of campaign finance violations
10/6/2016	Fancy Bears' Hack Team	Fancy Bears' Hack Team claims to leak emails from USADA
10/7/2016	WikiLeaks	WikiLeaks publishes 2,050 emails allegedly stolen from Clinton campaign chairman John Podesta, including excerpts from Clinton's Wall Street speeches; the dump is described as "part 1" by WikiLeaks
10/7/2016		The US Office of the Director of National Intelligence (DNI) and Department of Homeland Security (DHS) issue a joint statement declaring that the Russian Government was behind breaches of US political organizations that resulted in leaks by Guccifer 2.0, DC Leaks, and WikiLeaks ¹²²
10/9/2016		2nd US Presidential Debate
10/10/2016	WikiLeaks	WikiLeaks publishes "part 2" of Podesta emails
10/11/2016	WikiLeaks	WikiLeaks publishes "part 3" of Podesta emails
10/12/2016	WikiLeaks	WikiLeaks publishes "part 4" and "part 5" of Podesta emails
10/13/2016	WikiLeaks	WikiLeaks publishes "part 6" of Podesta emails
10/14/2016	WikiLeaks	WikiLeaks publishes "part 7" of Podesta emails
10/15/2016	WikiLeaks	WikiLeaks publishes "part 8" of Podesta emails, including Hillary Clinton's Goldman Sachs private paid speeches
10/16/2016	WikiLeaks	WikiLeaks publishes "part 9" of Podesta emails
10/17/2016	WikiLeaks	WikiLeaks publishes "part 10" of Podesta emails
10/18/2016	WikiLeaks	WikiLeaks publishes "part 11" of Podesta emails
10/18/2016	Guccifer 2.0	Guccifer 2.0 posts alleged DNC correspondence and documents discussing Donald Trump's finances, including copies of Trump's required Federal Election Commission (FEC) filings and plans to file Freedom of Information Act (FOIA) requests to discover additional information about the Republican candidate's finances
10/19/2016		3rd US Presidential Debate
10/19/2016	DC Leaks	DC Leaks provides the Daily Caller exclusive access to emails purportedly belonging to White House staffer Zachary Leighton ¹²³
10/19/2016	WikiLeaks	WikiLeaks publishes "part 12" of Podesta emails
10/20/2016	WikiLeaks	WikiLeaks publishes "part 13" of Podesta emails including emails from Barack Obama via his alleged personal email address
10/21/2016	DC Leaks	DC Leaks makes emails allegedly belonging to Sarah Stoll and Beanca Nicholson publicly available by removing the folders' password protections

¹²¹ <https://www.wada-ama.org/en/media/news/2016-10/cyber-security-update-wadas-incident-response>

¹²² <https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national>

¹²³ <http://dailycaller.com/2016/10/19/exclusive-hundreds-of-white-house-staffers-emails-get-leaked/>

10/21/2016	WikiLeaks	WikiLeaks publishes “part 14” of Podesta emails
10/22/2016	WikiLeaks	WikiLeaks publishes “part 15” of Podesta emails
10/22/2016	CyberBerkut	CyberBerkut claims to have leaked documents from the National Endowment for Democracy (NED) purportedly demonstrating that NED “sponsored a bloody civil war in Ukraine” working with reporter David Satter, who CyberBerkut claims orchestrated anti-Russian propaganda through Radio Liberty and Russian opposition media outlets.
10/23/2016	WikiLeaks	WikiLeaks publishes “part 16” of Podesta emails
10/24/2016	WikiLeaks	WikiLeaks publishes “part 17” of Podesta emails
10/25/2016	WikiLeaks	WikiLeaks publishes “part 18” of Podesta emails
10/26/2016	WikiLeaks	WikiLeaks publishes “part 19” of Podesta emails
10/27/2016	WikiLeaks	WikiLeaks publishes “part 20” of Podesta emails
10/28/2016	WikiLeaks	WikiLeaks publishes “part 21” of Podesta emails
10/29/2016	WikiLeaks	WikiLeaks publishes “part 22” of Podesta emails
10/29/2016	@anpoland	@anpoland claims to have leaked data from the Bradley Foundation; one of the leak announcements also contains the hashtag #HillaryDown, which is subsequently amplified through Warlist activity
10/29-11/1/2016	@anpoland	“Anti-Global,” “News,” “Breaking News,” “Question” Warlists promote Bradley Foundation leak
10/30/2016	WikiLeaks	WikiLeaks publishes “part 23” of Podesta emails
10/31/2016	DC Leaks	DC Leaks makes emails purportedly stolen from Zachary Leighton publicly available by removing the folder’s password protection
10/31/2016	WikiLeaks	WikiLeaks publishes “part 24” of Podesta emails; announces a “third phase” of leaks regarding US presidential election
11/1/2016	WikiLeaks	WikiLeaks publishes “part 25” of Podesta emails
11/2/2016	WikiLeaks	WikiLeaks publishes “part 26” of Podesta emails
11/2-3/2016	@anpoland	@anpoland-related “ClintonCorruption” Warlist activity promotes the Bradley Foundation leak
11/3/2016	WikiLeaks	WikiLeaks publishes “part 27” of Podesta emails
11/3/2016	WikiLeaks	WikiLeaks publishes “part 28” of Podesta emails, describing them as “DoJ/FBI/Human special”
11/3/2016	@anpoland	@anpoland claims to have conducted a DDoS attack against the Bradley Foundation
11/3/2016	@anpoland	@anpoland-related “ClintonCurruption [sic]” Warlist activity promotes the Bradley Foundation DDoS attack claim
11/4/2016	WikiLeaks	WikiLeaks publishes “part 29” and “part 30” of Podesta emails
11/4/2016	Guccifer 2.0	Guccifer 2.0 warns on Twitter and WordPress that “Democrats may rig the elections,” and calls on hackers to monitor the elections for signs of fraud

11/4/2016	CyberBerkut	CyberBerkut claims to have leaked documents allegedly belonging to Boris Lozhkin, the former head of the Ukrainian Presidential Administration, that allegedly demonstrate a conspiracy between the Kiev government and US State Department employees, whom the persona claims to be sympathetic to the US Democratic Party, to expose evidence regarding Paul Manafort's work with former Ukrainian President Yanukovich in order to provide Hillary Clinton a political advantage. At least some of the documents appear to have been fabricated.
11/5/2016	WikiLeaks	WikiLeaks publishes "part 31" of Podesta emails
11/6/2016	WikiLeaks	WikiLeaks publishes "part 32" of Podesta emails
11/6/2016	WikiLeaks	WikiLeaks publishes "8,263 emails from the DNC" accompanied by the hashtag #DNCLeak2
11/7/2016	WikiLeaks	WikiLeaks publishes "part 33" and "part 34" of Podesta emails
11/7/2016	WikiLeaks	WikiLeaks claims that their "email publication servers are under a targeted DoS attack since releasing #DNCLeak2"
11/8/2016		US Election Day
11/8/2016	@anpoland	@anpoland tweets messages expressing opposition to the Democratic Party and Hillary Clinton that include the hashtag #WarAgainstDemocrats." Subsequently, @anpoland "Russian Prostitute" and "GOP - WAR" Warlists attempt to trend the #WarAgainstDemocrats hashtag
11/9/2016	@anpoland	"Russian Prostitute" and "GOP - WAR" Warlists merge to become the "GOP - WON" Warlist, celebrate Bradley Foundation leak and Clinton electoral loss
11/22/2016	Fancy Bears' Hack Team	Fancy Bears' Hack Team tweets "we're still here," "#OpOlympics is under way," and "contact us," but does not announce any new threat activity
11/27/2016	CyberBerkut	CyberBerkut posts a transcript of an alleged phone call between former US Vice President Joe Biden and Ukrainian President Petro Poroshenko in which Biden purportedly claimed an International Monetary Fund (IMF) payment to Ukraine was linked to the nationalization of PrivatBank. CyberBerkut claims that this demonstrates that the US Government is controlling Ukrainian oligarchs. The authenticity of the transcript is unconfirmed.
12/1/2016	WikiLeaks	WikiLeaks posts documents from the German Bundestag inquiry into the relationship between Germany's Bundesnachrichtendienst (BND) and the US National Security Agency (NSA)
12/9/2016		WADA publishes Part II of the McLaren investigation report ¹²⁴
12/9/2016		President Obama orders a review of 2016 election hacking ¹²⁵
12/13/2016	Fancy Bears' Hack Team	Fancy Bears' Hack Team claims to leak additional emails from USADA and the Canadian Center for Ethics in Sport (CCES) that allegedly demonstrate that the US and Canada conspired against the International Olympic Committee (IOC) "to further their political interests"
12/16/2016	Fancy Bears' Hack Team	Fancy Bears' Hack Team actively solicits reporters to cover their leak activity, including one at Ars Technica ¹²⁶

¹²⁴ <https://www.wada-ama.org/en/media/news/2016-12/wada-publishes-independent-mclaren-investigation-report-part-ii>

¹²⁵ https://www.washingtonpost.com/world/national-security/obama-orders-review-of-russian-hacking-during-presidential-campaign/2016/12/09/31d6b300-be2a-11e6-94ac-3d324840106c_story.html?utm_term=.53eed3805dbb

¹²⁶ <http://arstechnica.com/security/2016/12/hackers-behind-anti-doping-leaks-please-write-about-us-well-give-you-exclusive/>

12/19/2016	DC Leaks	DC Leaks retweets WikiLeaks tweet on DNC "pied piper" strategy memo in which the Clinton campaign advised the DNC to encourage media coverage of "pied piper" Republican candidates such as Trump and Cruz in order to weaken the prospects of candidates viewed as potentially more competitive threats
12/29/2016		US CERT publishes "Grizzly Steppe - Russian Malicious Cyber Activity" report and indicators ¹²⁷
12/29/2016-01/10/2017	Fancy Bears' Hack Team	Fancy Bears' Hack Team announces a "Cartoon Competition," calling for "funny images on athletes with TUEs [sic]" tagged with the hashtag #DopingCartoon and stating that "the best cartoons will be posted as our profile photos on Twitter and Facebook for a week." The group subsequently posts a number of memes tagged #DopingCartoon and changes its profile picture
1/6/2017		DNI publishes Intelligence Community Assessment "Assessing Russian Activities and Intentions in Recent US Elections" ¹²⁸
1/10/2017		The Association of National Anti-Doping Organizations (NADOs) calls for a blanket ban on Russian athletes until faith has been restored in RUSADA ¹²⁹
1/12/2017	Guccifer 2.0	Guccifer 2.0 posts a blog criticizing the evidence presented in the US Government's recently publicly released Russian hacking reports
1/13/2017	CyberBerkut	CyberBerkut posts an image of an email allegedly exchanged between US officials revealing plans to falsify technical evidence in the US Government's December 2016 and January 2017 publicly released reports regarding Russian hacking and the 2016 presidential election. ¹³⁰ The authenticity of this email is unconfirmed, and would not be difficult to fabricate.
1/15/2017	CyberBerkut	CyberBerkut claims to have leaked mail from the Polish Consul, emails from the German police, and documents from the Ukrainian Ministry of Internal Affairs (MIA), though the post was subsequently deleted from the group's website and social media outlets.
1/15/2017	Fancy Bears' Hack Team	Der Spiegel publishes an article discussing anti-doping efforts based on WADA and USADA materials allegedly stolen and provided exclusively to the publication by Fancy Bears' Hack Team ¹³¹
1/16/2017	CyberBerkut	CyberBerkut claims to have leaked additional documents from the Ukrainian MIA, some of which relate to Interior Minister Arsen Avakov. Also among the leaked documents is at least one email exchanged between Ukrainian MIA employees and a Latvian police officer. One screenshot appears to show that the perpetrators have access to a Zimbra collaboration software administrator page, lending some credence to the authenticity of at least some of the documents. Information about this alleged compromise was also subsequently removed from CyberBerkut's websites and social media outlets.
1/18/2017	Fancy Bears' Hack Team	Fancy Bears' Hack Team promotes Der Spiegel article via Twitter
1/26/2017	Fancy Bears' Hack Team	Fancy Bears' Hack Team promotes a BBC article that referenced leaked TUEs ¹³²
2/21/2017	APT28	APT28 gains access to International Association of Athletics Federations (IAAF) networks, according to IAAF ¹³³

¹²⁷ <https://www.us-cert.gov/security-publications/GRIZZLY-STEPPE-Russian-Malicious-Cyber-Activity>

¹²⁸ https://www.dni.gov/files/documents/ICA_2017_01.pdf

¹²⁹ <http://www.reuters.com/article/us-sport-doping-nado-russia-idUSKBN14U2FT>

¹³⁰ <https://twitter.com/cyberberkut2/status/819887266650853377>

¹³¹ <http://www.spiegel.de/international/world/sports-doping-and-the-difficult-fight-to-prevent-it-a-1129918.html>

¹³² <http://www.bbc.com/sport/cycling/38728410>

¹³³ <https://www.iaaf.org/news/press-release/iaaf-cyber-attack>

2/26/2017	Fancy Bears' Hack Team	The Sunday Times publishes an article about doping allegations related to a track and field training program and associated athletes based on alleged USADA documents stolen by "Fancy Bears" ¹³⁴
3/3/2017	Fancy Bears' Hack Team	Fancy Bears' Hack Team tweets quote from the director of the French Athletics Federation stating "Taking drugs when you are not sick is clearly entering into foundations for doping"
3/4/2017	Fancy Bears' Hack Team	Der Spiegel publishes an article discussing doping allegations related to a track and field training program based on the same alleged USADA documents referenced in The Sunday Times article ¹³⁵
3/6/2017	Fancy Bears' Hack Team	Fancy Bears' Hack Team publishes tweets referencing The Sunday Times and Der Spiegel, likely to draw attention to the articles and to call attention to allegations of athlete "doping"
3/17/17	Fancy Bears' Hack Team	Der Spiegel publishes an article discussing doping allegations of soccer players based on a "WADA spreadsheet" provided to the publication by Fancy Bears' Hack Team ¹³⁶
4/3/2017	APT28	IAAF discloses that it was compromised by APT28 beginning on February 21, 2017 ¹³⁷
4/20/2017	Fancy Bears' Hack Team	BBC Sport publishes an article about an impending review of British Cycling's practices following the delivery of a suspicious package addressed to a British cyclist ¹³⁸
4/26/17	CyberBerkut	Pro-Russian Government media outlet LIFE posts a document allegedly stolen by CyberBerkut that discussed an incident in which a schoolboy traded alcohol for a grenade with a Ukrainian soldier. ¹³⁹ No official CyberBerkut outlets reported this incident.
5/19/2017	Fancy Bears' Hack Team	The New York Times publishes an article discussing doping allegations related to a track and field training program documented in a report Fancy Bears' Hack Team claims to have stolen from USADA. ¹⁴⁰
5/23/2017	Fancy Bears' Hack Team	Fancy Bears' Hack Team publishes tweets referencing the May 19, 2017, New York Times article discussing the allegedly leaked USADA report about a track and field training program as well as an April 20, 2017 BBC article discussing doping allegations for a British cyclist.
7/5/17	Fancy Bears' Hack Team	Fancy Bears' Hack Team claims to leak data from IAAF regarding alleged athlete doping violations and other purported unfair behavior by anti-doping bodies.
7/12/17	CyberBerkut	CyberBerkut claims to leak emails from the Head of the Board of a Ukrainian NGO that allegedly reveal links between a Ukrainian money laundering operation and Hillary Clinton's campaign funds.
8/23/17	CyberBerkut	CyberBerkut claims to leak emails from the head of a Kiev-based NGO that allegedly demonstrate that the US tests biological weapons in Ukraine. Among the leaked emails, we observed what appeared to be four phishing messages, which we linked to tactics and phishing infrastructure controlled by APT28.

¹³⁴ <http://www.thetimes.co.uk/article/leaked-doping-report-says-mo-was-given-risky-treatment-65nxsvmhs>

¹³⁵ <http://www.spiegel.de/sport/sonst/nike-oregon-project-usada-erhebt-schwere-vorwurfe-gegen-weltklasselaeufer-a-1137247.html>

¹³⁶ <http://www.spiegel.de/international/zeitgeist/football-rife-with-performance-enhancing-drugs-a-1139238.html>

¹³⁷ <https://www.iaaf.org/news/press-release/iaaf-cyber-attack>

¹³⁸ <http://www.bbc.com/sport/cycling/39654790>

¹³⁹ https://life.ru/t/%D0%BD%D0%BE%D0%B2%D0%BE%D1%81%D1%82%D0%B8/1002554/kibierbierkut_vsu_mieniajut_niesoviershiennolietnim_alkoghol_na_oruzhiie

¹⁴⁰ <https://www.nytimes.com/2017/05/19/sports/nike-oregon-project-alberto-salazar-dathan-ritzenhein.html>